UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

MAESTRIA EN TELEMÁTICA

PROYECTO DE TESIS

DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COMPAÑÍA ACOTECNIC Cía. Ltda. BASADO EN LA NORMA NTE INEN ISO/IEC 27002

PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN TELEMÁTICA

AUTOR: Ing. Darwin Stalin Lanche Capa

DIRECTOR: Ing. Alcides Fabián Araujo Pacheco, MgT.

CUENCA-ECUADOR
2015

Resumen

Al ser la información un bien valioso para las empresas, debe estar debidamente protegida mediante políticas de seguridad que permitan una adecuada gestión de la seguridad de la información. Una correcta administración de las Tecnologías de la Información y Comunicación (TICs), una cultura de ética en el manejo y cuidado de la información, y un correcto modelo administrativo, basado en los objetivos claros y la legislación vigente, puede proteger los intereses de la empresa, asegurando la continuidad del negocio.

Partiendo de la necesidad de determinar la factibilidad de implementar un sistema de seguridad de la información, en pequeñas empresas, el presente proyecto de tesis propone analizar el estado de una empresa local dedicada a brindar servicios profesionales en el área de la consultoría técnica, y, con estos resultados, establecer un esquema que se pueda seguir para implementar, mejorar y mantener un sistema de gestión de seguridad de la información óptimo, acorde con los requerimientos e inversión que ésta pueda hacer.

Se hace un análisis en base a las mejores prácticas recomendadas por la norma NTE INEN ISO/IEC 27002, en cada una de las áreas y las TICs que la empresa dispone para el desarrollo de sus actividades diarias.

Palabras Claves: Tecnologías de la Información y Comunicación (TICs), Sistema de seguridad de la información, Sistema de gestión de seguridad de la información, norma NTE INEN ISO/IEC 27002.

Abstract

Being a valuable benefit for business, the information, must be properly protected through security politics that lend us an appropriate management of information security. A correct administration of the Information and Communication Technologies (ICT), a culture of ethicsin the management and care of the information, and a correct model of administration, based in clear objectives and the current legislation, may protect the interest of the company, ensuring the continuity of this business.

Setting off the need to determinate the feasibility of implementing an information security system, in small companies, the current thesis project proposes analyzing the condition of a local company dedicated to offer professional services in the technical consultancy area, and with these results, establish a schema that can be followed to implement, improve and maintain an optimal security management system, in accordance to the requirements and investment that it can provide.

An analysis based on the best practices recommended by the policy NTE INEM ISO/IEC 27002 is made, in every single area of the ICT that the company possesses for the development of their daily activities.

Key Words: Information and Communication Technologies (ICT), Information security system, Security management system, Policy NTE INEM ISO/IEC 27002

Índice de Contenidos

Darwin Stalin Lanche Capa, autor/a de la tesis “DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COMPAÑÍA ACOTECNIC Cía. Ltda. BASADO EN LA NORMA NTE INEN ISO/IEC 27002”, reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Master en Telemática. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor/a

Cuenca, 28 de mayo de 2015

Darwin Stalin Lanche Capa

C.I: 1103556633

Darwin Stalin Lanche Capa, autor/a de la tesis “DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COMPAÑÍA ACOTECNIC Cía. Ltda. BASADO EN LA NORMA NTE INEN ISO/IEC 27002”, certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

Cuenca, 28 de mayo de 2015

Darwin Stalin Lanche Capa

C.I: 1103556633

AGRADECIMIENTOS

A la Universidad de Cuenca por la oportunidad brindada para culminar los estudios de Maestría, en especial a los Señores Directores de Postgrados, Director de la Maestría y Director del Programa Especial de Titulación, docentes y personal de apoyo.

A la Compañía Asociación de Consultores Técnicos Acotecnic Cia. Ltda., por la apertura brindada para la ejecución del presente proyecto de investigación, en particular a sus Directivos y al personal del Departamento de Sistemas y Sistemas de Información Geográfica.

Un sincero agradecimiento al Ing. Alcides Araujo P., por el valioso aporte brindado durante la dirección del presente estudio.

Darwin S. Lanche C.

DEDICATORIA

A mi familia, mi esposa Ginna y mis hijas Anita Victoria y Amelia Martina, por compartir conmigo los logros, fruto de nuestro esfuerzo y sacrificio.

Darwin S. Lanche C.

CAPÍTULO I

Introducción, Objetivos, Alcance

1.1 Definición del Tema

Diseño de un Sistema de Seguridad de la Información para la Compañía Asociación de Consultores Técnicos ACOTECNIC Cía. Ltda., basado en la Norma NTE INEN ISO/IEC 27002.

1.2 Antecedentes y Definición del Problema

En la actualidad, el acceso a la información de las instituciones a través de su red, es relativamente fácil con las herramientas disponibles y de libre obtención en internet.La ausencia de un nivel de seguridad de información efectivo, provoca que las Tecnologías de la Información y Comunicación (TICs) que utiliza no sean confiables, además de debilidades en la protección para el hardware y la autentificación de usuarios para el manejo de cierta información.

El aplicar controles para la protección de los datos de una forma adecuada, resulta imprescindible; sin embargo es importante además, analizar los tipos de controles adecuados para cada empresa.

Ante la necesidad de determinar la factibilidad de implementar un Sistema de Seguridad de la Información en pequeñas empresas, se propone analizar el estado de una empresa local dedicada a brindar servicios profesionales en el área de la consultoría técnica.

Para evaluar la conveniencia de la implementación de Sistemas de Seguridad de la Información en pequeñas empresas, se ha invitado a ACOTECNIC Cía. Ltda., para que forme parte de esta investigación, ya que su accionar permite analizar varios escenarios para el manejo de la información:

a. Información base entregada por las empresas contratantes.
b. Información generada en cada área especializada de los proyecto.

c. Comunicaciones remotas entre las diferentes sucursales de la empresa y sus proveedores.
d. Entrega de resultados de los estudios ejecutados.

ACOTECNIC Cía. Ltda., es una compañía con considerable experiencia, que opera en nuestro País desde el año 1994; desarrolla sus actividades de Consultoría Técnica en el área de la Ingeniería. Su oficina matriz se encuentra en la ciudad de Cuenca. Ha colaborado en importantes proyectos tanto para entidades públicas y privadas, además ha trabajado en forma conjunta con empresas extranjeras. Su misión es desarrollar soluciones adecuadas, estratégicamente planteadas por un equipo de especialistas profesionales de amplia trayectoria, lo que les permite ofrecer a sus clientes finales una solución óptima, producto de la investigación, el desarrollo y mejora permanente de los procesos internos.
Sus soluciones, que parten desde evaluaciones preliminares, hasta la puesta en marcha de proyectos, han sido requeridas a nivel nacional, por lo que actualmente operan con oficinas sucursales en Guayaquil y Quito. Dependiendo de las necesidades, han tenido que operar desde otras ciudades, estableciendo oficinas temporales, o de forma remota, al realizar trabajos con especialistas en campo. [1]

1.3 Justificación del Problema

La información es un bien intangible para las empresas. El disponer de la información adecuada, en determinado momento, puede generar una ventaja competitiva que marque la diferencia en el desarrollo de las actividades y el crecimiento de la misma.

Cualquiera sea la forma o medio en el que esté almacenada o compartida la información, debe estar debidamente protegida. En términos generales, una correcta administración de las TICs, apoyado en políticas de seguridad definidas, sumado a una cultura de ética en el manejo y cuidado de la

[1] Fuente: www.acotecnic.com

información, pueden proteger los intereses de la empresa, asegurando la continuidad del negocio.

Las grandes empresas, debido al capital económico con el que cuentan, pueden mantener dentro de su nómina, a profesionales que se encarguen del manejo y gestión de la seguridad de la información GSI, así como disponer de los recursos tecnológicos adecuados para esta tarea. Al otro extremo, las pequeñas empresas, en muchas ocasiones por desconocimiento, no destinan recursos para implementar un sistema de seguridad de la información que garantice la integridad, confidencialidad y disponibilidad de la misma; generalmente operan con redes de comunicación elementales, que cumplen solo con la función de conectar sus equipos de computación, tampoco cuentan con políticas claras para el manejo y cuidado de la información. Su accionar se ha vuelto una actividad reactiva a los eventos ocurridos cuando pueden poner en riesgo la continuidad del negocio.

1.4 Planteamiento de Objetivos

1.4.1 Objetivo General

Establecer los lineamientos a seguir para implementar las recomendaciones de la norma de seguridad de la información NTE INEN ISO/IEC 27002 en pequeñas empresas mediante el análisis de un caso real.

1.4.2 Objetivos Específicos

- Brindar un diagnóstico del estado de la seguridad de la información en la Compañía, mediante el levantamiento de información y las políticas existentes relacionadas a la seguridad de la información.

- Determinar los riesgos existentes para el Sistema de Seguridad de la Información, en base a las recomendaciones dadas por la normativa NTE INEN ISO/IEC 27002.
- Determinar las amenazas debido al factor humano y definir una estrategia para cambiar comportamientos que pudieran afectar al sistema de gestión de seguridad de la información.
- Plantear los lineamientos base para determinar las políticas de seguridad más convenientes para la Compañía.

1.5 Alcance

Este trabajo y los lineamientos que en él se proponen para la implementación de un sistema de seguridad de la información [2] basado en la en la Norma NTE INEN ISO/IEC 27002, para una pequeña empresa, pretende evaluar mediante un análisis de riesgos la conveniencia de la implementación de los controles que recomienda la norma en este tipo de empresas.

La investigación se centra en el análisis de las políticas y prácticas actuales que son manejadas por la compañía ACOTECNIC Cía. Ltda., en lo referente a la seguridad de la información, para el desarrollo de sus actividades diarias. El plan de seguridad propuesto, basará su estructura en políticas, controles y medidas de prevención, y corrección de posibles riesgos a los activos de la Compañía; además de proteger la confidencialidad, disponibilidad e integridad de la información y datos.

1.6 Enumeración de los Entregables

- Memoria del Sistema de Seguridad de Información Implementado.
- Resultado de la evaluación acerca del Sistema de Seguridad para ACOTECNIC Cía. Ltda.
- Memoria de Tesis.

[2] Sistema de Seguridad de la Información: Conjunto de estrategias y recomendaciones a ser implementadas para mejorar la seguridad de la información. Concepto utilizado por el autor para el desarrollo del presente trabajo de investigación.

CAPÍTULO II

MARCO TEÓRICO

A continuación se proporcionarán conceptos básicos que se utilizarán durante el desarrollo del proyecto. Nos ayudarán a comprender la importancia de la seguridad de la información; las amenazas y riesgos a los que están expuestos los datos; y nos permitirá conocer acerca de serie de normas ISO/IEC 27000 y de la normativa NTE INEN ISO/IEC 27002.

1. Términos [3]

1.1 Activo: Algo que tenga valor para lo organización.

1.2 Control: Herramienta de la gestión del riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

1.3 Evento de seguridad de información: Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

1.4 Incidente de seguridad de información: Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.

1.5 Política: Dirección general y formal expresada por la gerencia.

1.6 Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

[3] Citado textualmente de la Norma Técnica NTP-ISO/IEC 17799

1.7 Terceros: Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.

1.8 Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

1.9 Vulnerabilidad: Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

1.10 Información

La información es considerada como uno de los activos más importante para el desarrollo del negocio de una organización. La información puede existir en muchas formas: Impresa, escrita, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en una película o hablada en una conversación; cualquiera que sea la forma, debe ser protegida adecuadamente. [4]

1.11 Elementos de la Información [5]

Los elementos de información son todos los componentes que generan, contienen, mantienen o guardan información; también son llamados activos o recursos. Para impedir daños a la empresa es vital evitar su pérdida, modificación o el uso inadecuado de su contenido.

Generalmente se distinguen tres grupos de elementos:

- **Datos e Información**: Son los datos como tal.
- **Sistemas e Infraestructura**: Son los componentes donde se generan, mantienen o guardan los datos.

[4] National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 2000

[5] https://protejete.wordpress.com/gdr_principal/elementos_informacion/. Título: Gestión de Riesgo en la Seguridad Informática. Fecha de ingreso: Febrero 2015

- **Personal**: Son todos los individuos que manejan o tienen acceso a los datos, constituyen los activos más difíciles de manejar, porque son móviles, pueden cambiar con cierta frecuencia y son impredecibles en su comportamiento.

Podemos mencionar algunos componentes dentro de cada grupo de elementos:

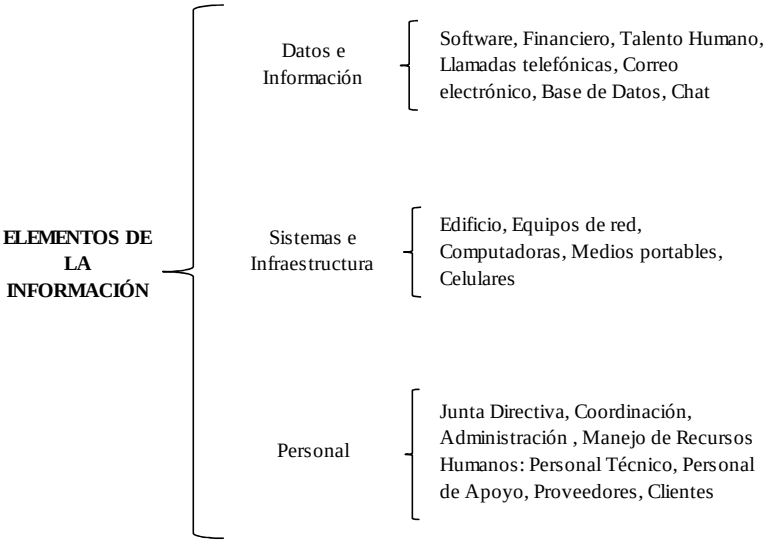


Figura 2.1: Elementos de la Información
Fuente: Editado de proteje.wordpress.com

1.12 Amenazas a la Seguridad de la Información [6]

Actualmente el desarrollo de las tecnologías de la información y comunicación TICs han facilitado el cumplimiento de las actividades de las empresas, sin embargo éste mismo desarrollo ha aumentado el riesgo al que está expuesta la información debido a la aparición de nuevas amenazas.

Una amenaza es todo evento o acción capaz de atentar contra la seguridad de la información de forma material o inmaterial.

[6] Fuente: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12. Título: Universidad Nacional de Luján – Buenos Aires Argentina. Fecha de ingreso: Febrero 2015

Sólo puede existir amenaza si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Situaciones, tales como el incremento y el perfeccionamiento de las técnicas de trashing, ingeniería social, ingeniería social inversa, ataques de monitorización, de escaneo o de modificación, Denial of Service DoS [7], la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

En los sistemas de información es donde la mayor parte de la información procesada o no procesada es resguardada, ya sea en equipos informáticos, soportes de almacenamiento y redes de datos. Estos sistemas de información son activos que están sujetos a vulnerabilidades y amenazas que pueden provenir desde el interior de la empresa como desde el exterior.

1.12.1 Tipos de amenazas

Las amenazas pueden clasificarse en dos tipos: [8]

- Intencionales, en caso de que deliberadamente se intente producir un daño mediante ataques activos (por ejemplo el robo, modificación o destrucción de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
- No intencionales, en donde se producen acciones u omisiones de acciones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).

El siguiente gráfico representa los tipos de amenazas:

[7] Referirse al Glosario de Conceptos Técnicos página 149
[8] Fuente: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12. Título: Universidad Nacional de Luján – Buenos Aires Argentina. Fecha de ingreso: Febrero 2015

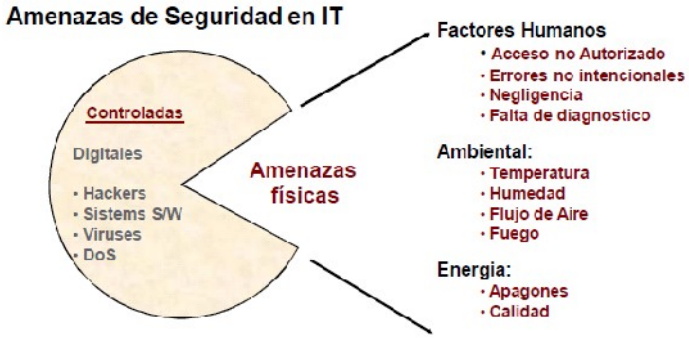


Figura 2.2: Amenazas de Seguridad
Fuente: http://www.gitsinformatica.com/basico%20empresa.html
Protección básica de la Empresa en las TIC

1.12.2 Ataques activos

Considerando el flujo normal de comunicación entre el emisor y receptor, los ataques activos tienen como objetivo apoderarse, detener, dañar o destruir la información. Entre los ataques más comunes están:

Interrupción: Cuando el objetivo es detener el flujo de comunicación evitando que la información llegue al receptor.

Intercepción: Cuando el objetivo es apoderarse del flujo de comunicación, pero a diferencia de la interrupción el mensaje finalmente es enviado al receptor.

Modificación: Cuando el mensaje original es alterado llegando al receptor de forma alterada.

Fabricación: Cuando el atacante envía un mensaje al receptor con el objetivo de hacerle creer que es el emisor.

Destrucción: Cuando el mensaje es destruido evitando que llegue al receptor.

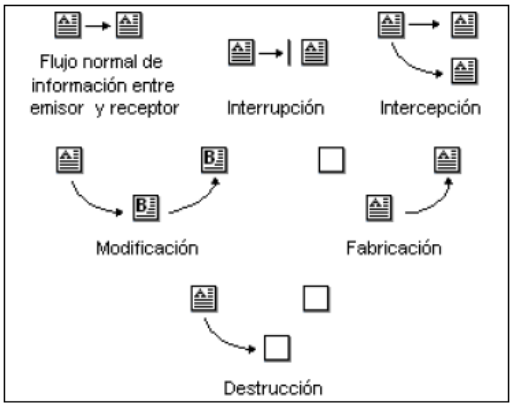


Figura 2.3: Tipo de ataques a activos
Fuente: CERT, Software Engineering Institute-www.cert.org
Elaborado por: Howard, John D.

1.13 Seguridad de la Información

La definición para el término Seguridad Informática ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la "International Organization for Standardization" (ISO) y por la "International Electrotechnical Commission" (IEC).

"La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio." [9]

La seguridad es un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se puede gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

Para conseguir la seguridad de la información se definen un conjunto de controles efectivos, que pueden ser políticas, manual de funciones, procedimientos, estructuras organizativas, planes de contingencia y funciones

[9] Fuente: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1. Título: Observatorio Tecnológico. Autor: Elvira Mifsud. Fecha de ingreso: Diciembre 2014

de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados permanentemente, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

Es necesario además, realizar una evaluación de riesgos periódicamente estableciendo un punto de equilibrio en relación de costo–beneficio.

En la siguiente gráfica que representa la relación costo – nivel de seguridad: A mayor seguridad, se logra reducir significativamente los riesgos a los que está expuesta la información; sin embargo, los costos también se incrementan. Es por ello que cada empresa debería encontrar el punto de equilibrio adecuado para sus necesidades y de acuerdo a su capacidad económica.

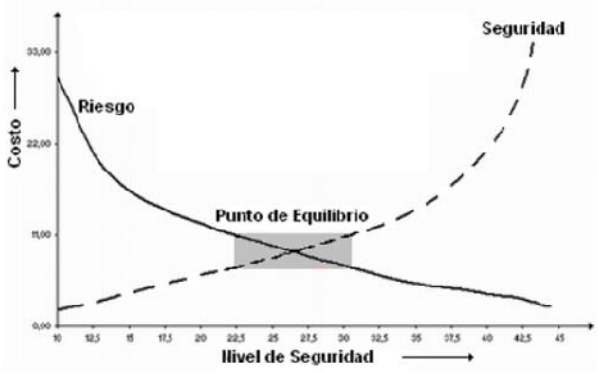


Figura 2.4: Punto de equilibrio costo – seguridad [10]

En el caso de pequeñas empresas el aspecto económico es el factor más importante al momento de elegir las estrategias a implementarse. Por lo que es sumamente importante concientizar a los Directivos de la Compañía sobre la importancia de la seguridad de la información y de la identificación de las vulnerabilidades más críticas.

[10] Fuente: http://www.segu-info.com.ar/ataques/tipos.htm. Título: SeguInfo Seguridad de la Información. Autor: Cristian Borghello. Fecha de ingreso: Marzo 2015

1.13.1 Bases de la Seguridad de la Información [11]

Es imposible definir un sistema como absolutamente seguro, más bien se califica como fiable [12].En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- **Confidencialidad**: Acceso a la información solo mediante autorización y de forma controlada.
- **Integridad**: Modificación de la información solo mediante autorización.
- **Disponibilidad**: La información del sistema debe permanecer accesible mediante autorización.

La figura 2.5 muestra la trilogía de: Confidencialidad, Integridad y Disponibilidad, que además son pilares de la propia norma ISO/IEC 27001. Debe enmarcarse entonces en el contexto del negocio, del marco legal y la estrategia empresarial.[13]

[11] Fuente: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1. Título: Observatorio Tecnológico. Autor: Elvira Mifsud. Fecha de ingreso: Diciembre 2014

[12] Referirse al Glosario de Conceptos Técnicos página 149

[13] Tesis: Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Autor: Ing. Gustavo Pallas Mega. Fecha: Montevideo, Uruguay - Diciembre2009.

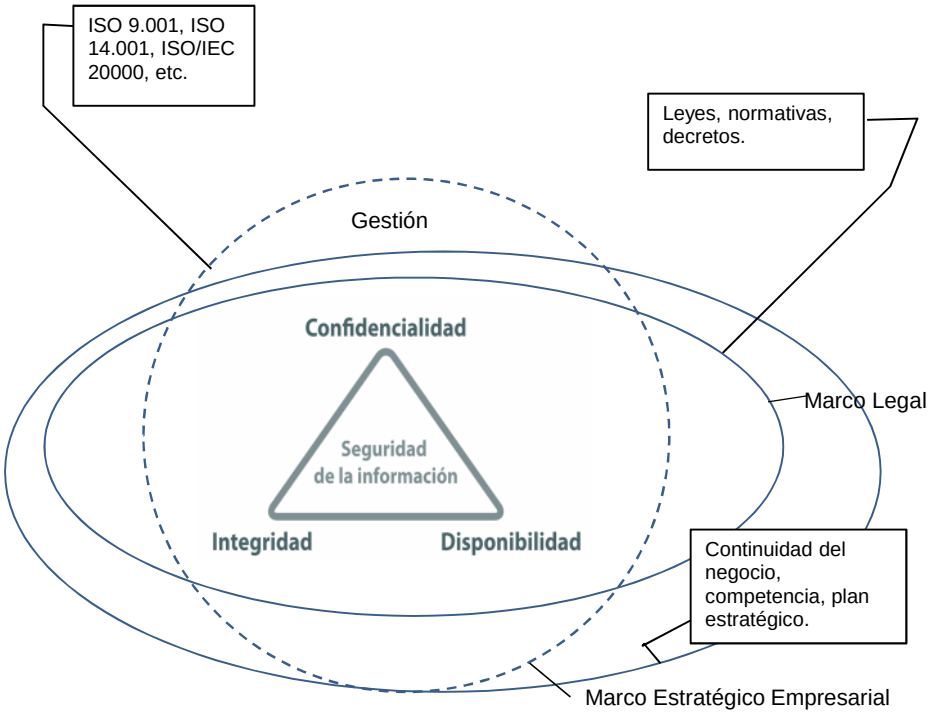


Figura 2.5: Pilares Fundamentales de la Seguridad de la Información [14]

Otras características de la seguridad de la información podrían ser:

- **Autenticidad**: Asegura el origen de la información, la identidad de usuarios al momento de un acceso debe ser validada, de modo que se puede demostrar que es quien dice ser.

- **No-repudio**: Imposibilidad de negación ante terceros del envío y/o recepción por parte del emisor y/o receptor de la información.

- **Trazabilidad**: Es el conjunto de acciones, medidas y procedimientos técnicos que permite autenticar y registrar la información desde que esta es enviada al usuario hasta que este último la recibe.

[14] Tesis: Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Autor: Ing. Gustavo Pallas Mega. Fecha: Montevideo, Uruguay - Diciembre2009.

1.13.2 Requisitos de seguridad

La organización debe identificar sus requisitos de seguridad. Se podría agrupar en tres requisitos principales.

- El primer requisito se enfoca en los objetivos y estrategias generales del negocio la cual permite realizar la valoración de los riesgos de la organización, con este requisito se identifican las amenazas de los activos, se calcula la vulnerabilidad y la probabilidad de su ocurrencia para realizar una probabilidad de su posible impacto en el negocio.

- EL segundo requisito es el conjunto de requisitos legales, estatutos, regulaciones y contratos que satisface a la organización, sus accionistas, socios comerciales y los proveedores.

- El tercer requisito está basado en los principios, objetivos y requisitos del tratamiento de la información que la organización ha desarrollado para sus operaciones.

1.13.3 Punto de partida de la seguridad de la información [15]

Los puntos de partida de la seguridad de la información se los divide en dos grandes grupos:

1. Controles desde el punto de vista legislativo.
    a) Protección de los datos de tipo personal.
    b) Salvaguardas de los requisitos de la organización.
    c) Derechos de propiedad privada.

2. Controles de mejores prácticas habituales.

[15] Fuente: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1. Título: Observatorio Tecnológico. Autor: Elvira Mifsud. Fecha de ingreso: Diciembre 2014

a) Documentación de la política de seguridad de la información.
b) Asignación de responsabilidades.
c) Formación y capacitación
d) Procedimiento correcto en las aplicaciones.
e) Gestión de la vulnerabilidad técnica
f) Gestión de la continuidad del negocio
g) Registro de las incidencias de seguridad y las mejoras

1.14 Política de Seguridad

Una política de seguridad es una técnica para gestionar los activos de una empresa para protegerlos apropiadamente, informando lo que está permitido, y qué no lo está; así como la responsabilidad de protección de los recursos que debería tener el personal.

"Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Esta a su vez establece las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos." [16]

El objetivo principal de las políticas de seguridad es proteger, prevenir y gestionar a una empresa, de las vulnerabilidades y riesgos a los que está expuesta; mediante normas, reglas y procedimientos precisos.

La certificación ISO 17799 define una política de seguridad como un documento que ofrece instrucciones de administración y soporte para la seguridad de la información de acuerdo con los requisitos empresariales y las leyes y reglamentaciones relevantes.

[16] Fuente: Análisis e Implementación de la Norma ISO 27002 para el Departamento de Sistemas de La Universidad Politécnica Salesiana Sede Guayaquil. Autores: Sr. Daniel Romo Villafuerte
Sr. Joffre Valarezo Constante

1. ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional.

La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). [BA07]

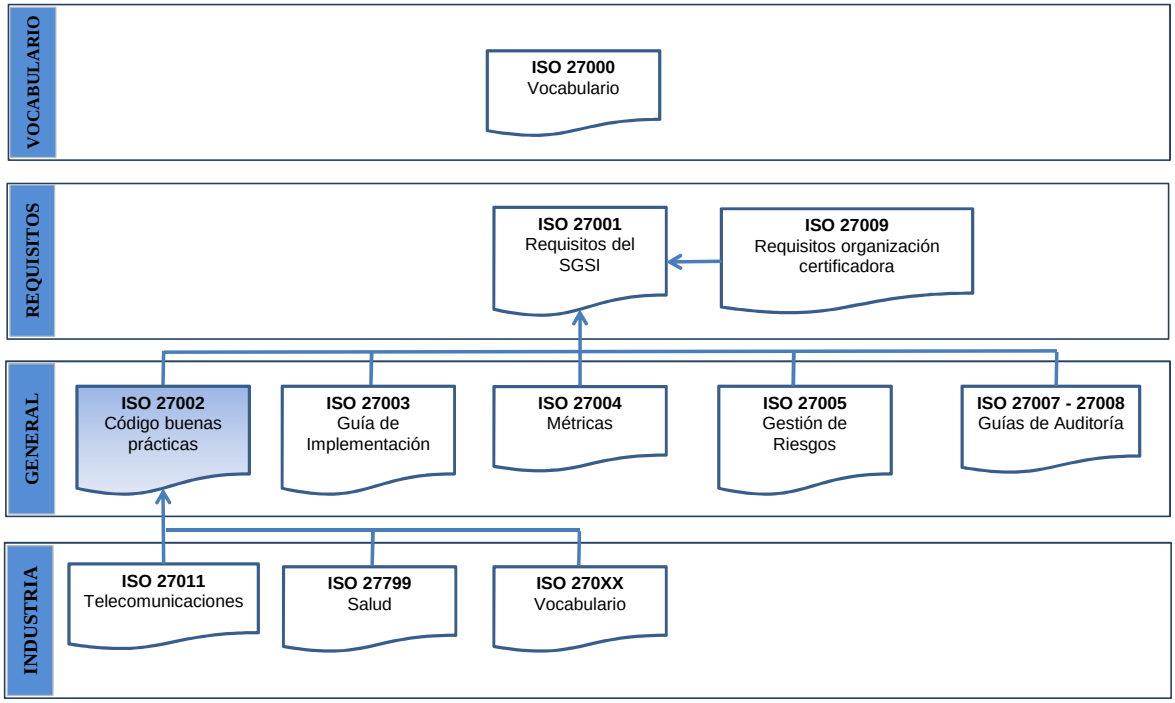


Figura 2.6: Familia de normas de Seguridad de la Información ISO 27000 [17]

El presente trabajo de investigación se basará en la norma NTE INEN ISO/IEC 27002

[17] Implementación de la norma ISO27001. Autor: Ing. Maurice Frayssinet Delgado, mfrayssinet@pcm.gob.pe /www.ongei.gob.pe. Oficina Nacional de Gobierno Electrónico e Informática. Perú

2.1 Normativa de Seguridad de la Información en el Ecuador.

Con el apoyo de varios ministerios e instituciones del sector público, desde el año 2010, se ha procurado definir los lineamientos que regularicen la implementación de SGSI en nuestro País.

De esta forma, de acuerdo a la información que se muestra en la página web del Instituto Ecuatoriano de Normalización (INEN), en el periodo 2010-2011 el subcomité técnico de "Tecnologías de la Información" había propuesto al menos siete normas de la familia ISO/IEC 27000 para que sean adoptadas como normativa ecuatoriana, las cuales han sido revisadas por los Ministerios de Telecomunicaciones, Ministerio de Industrias y Productividad, Subsecretaría de Industrias, Productividad e Innovación Tecnológica.

Mediante acuerdos ministeriales publicados en el Registro Oficial No. 804 del 29 de julio de 2011 y No. 837 del 19 de agosto de 2011, La Secretaría Nacional de Administración Pública crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación. Dentro de sus atribuciones tiene la responsabilidad de establecer los lineamientos de seguridad informática, protección de infraestructura computacional, incluyendo la información contenida, para las entidades de la Administración Pública Central e Institucional. En respuesta a esta tarea, la Comisión desarrolla el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la Norma NTE INEN ISO/IEC 27002 (Traducción de la norma ISO/IEC 27002).

El EGSI establece un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la administración pública.

Con estos antecedentes y contando con una normativa nacional vigente, el Gobierno Ecuatoriano, dispone a las entidades de la administración pública central, institucional y que dependen de la función ejecutiva, el uso obligatorio de las normas técnicas ecuatorianas serie NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. Esta disposición fue publicada en el Segundo Suplemento del Registro Oficial 088 del 19 de septiembre de 2013.

La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

La entidad encargada de realizar el seguimiento y control anual, o cuando las circunstancias lo ameriten, será la Secretaría Nacional de la Administración Pública, de conformidad a los lineamientos de la norma INEN ISO/IEC 27002 y sus futuras modificaciones, lo que implica que las entidades de la Administración Pública y que dependen de la Función Ejecutiva deberán realizar una evaluación, una adecuación o implementación, un seguimiento y una mejora continua sobre sus Sistemas de Gestión de Seguridad de la Información.

Una de las primeras Instituciones públicas en implementar esta normativa en nuestro País, es la Corporación Nacional de Telecomunicaciones con su proyecto “Diseño e implementación del Sistema de Gestión de Seguridad de la Información” (SGSI) aplicado al proceso: Venta e instalación de productos y servicios de datos e internet para clientes corporativos”.

2.2 Norma NTE INEN ISO/IEC 27002

2.2.1 Descripción General de la Norma

La Norma Técnica Ecuatoriana NTE INEN ISO/IEC 27002, elaborada por el Subcomité Técnico de "Tecnologías de La Información" en base a la norma ISO/IEC 27002, es una recopilación de las mejores prácticas para la Gestión de Seguridad de la Información.

Una vez que se han determinado los requerimientos de seguridad, se deben seleccionar los controles apropiados que deben implementarse para asegurar que los riesgos se reduzcan a un nivel aceptable.

La Norma NTE INEN ISO/IEC 27002 contiene un total de 133 controles que se distribuyen en once secciones principales. Algunos autores también nombran a estas secciones como dominios o cláusulas y son los siguientes:

1. Política de Seguridad de la Información.

2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Cada sección, tiene claramente definido sus objetivos de control. Para cumplir dichos objetivos, se especifican los distintos controles recomendados en base a las mejores prácticas relacionadas a la seguridad de la información.

Dependiendo del sector, la actividad y el alcance que la organización quiera dar a su Sistema de Seguridad de la Información, se debe definir cuantos controles serán realmente aplicados.

2.2.2. Estructura de la Norma NTE INEN ISO/IEC 27002 [18]

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo.

Cláusulas: Cada cláusula contiene un número de categorías principales de seguridad.

Categorías principales de seguridad:

Cada categoría principal de seguridad contiene:

a) Un objetivo de control declarando lo que se debe alcanzar.

b) Uno o más controles que pueden ser aplicados para alcanzar el objetivo de control.

[18] Fuente: Norma Técnica NTP-ISO/IEC 17799

Las descripciones del control son estructuradas de la siguiente manera:

Control: Define específicamente la declaración de control para satisfacer el objetivo de control.

Guía de implementación: Provee información más detallada para apoyar la implementación del control y conocer el objetivo de control. Algunas guías pueden no ser convenientes para todos los casos, por lo tanto algunas otras formas de implementar el control pueden ser más apropiadas.

Otra información: Provee información adicional que pueda ser necesaria, por ejemplo consideraciones legales y referencias de otros estándares.

El siguiente listado es un resumen de las recomendaciones que contiene la Norma. Estas recomendaciones están organizadas de la siguiente forma: En el primer nivel se mencionan las Cláusulas, en el segundo nivel se enlistan los Categorías Principales de Seguridad y en el tercer nivel del listado se mencionan los Controles Recomendados.

Para una mejor referencia, se han mantenido los números de capítulos y subcapítulos con que están identificados cada ítem dentro de la Norma ISO/IEC 27002

5. POLÍTICA DE SEGURIDAD.
5.1 Política de seguridad de la información.
5.1.1 Documento de política de seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.
6.1 Organización interna.
6.1.1 Compromiso de la Dirección con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información.
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
6.1.5 Acuerdos de confidencialidad.
6.1.6 Contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés.
6.1.8 Revisión independiente de la seguridad de la información.
6.2 Terceros.
6.2.1 Identificación de los riesgos derivados del acceso de terceros.

10.6.2 Seguridad de los servicios de red.
10.7 Manipulación de los soportes.
10.7.1 Gestión de soportes extraíbles.
10.7.2 Retirada de soportes.
10.7.3 Procedimientos de manipulación de la información.
10.7.4 Seguridad de la documentación del sistema.
10.8 Intercambio de información.
10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Soportes físicos en tránsito.
10.8.4 Mensajería electrónica.
10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
10.10.6 Sincronización del reloj.
11. CONTROL DE ACCESO.
11.1 Requisitos de negocio para el control de acceso.
11.1.1 Política de control de acceso.
11.2 Gestión de acceso de usuario.
11.2.1 Registro de usuario.
11.2.2 Gestión de privilegios.
11.2.3 Gestión de contraseñas de usuario.
11.2.4 Revisión de los derechos de acceso de usuario.
11.3 Responsabilidades de usuario.
11.3.1 Uso de contraseñas.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.2 Autenticación de usuario para conexiones externas.
11.4.3 Identificación de los equipos en las redes.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.
11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
12.1 Requisitos de seguridad de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad.
12.2 Tratamiento correcto de las aplicaciones.
12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.
12.3 Controles criptográficos.
12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.
12.4 Seguridad de los archivos de sistema.
12.4.1 Control del software en producción.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.
12.5 Seguridad en los procesos de desarrollo y soporte.
12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Control de las vulnerabilidades técnicas.
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13.1 Notificación de eventos y puntos débiles de seguridad de la información.
13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.
13.2 Gestión de incidentes y mejoras de seguridad de la información.
13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la continuidad del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
15. CUMPLIMIENTO.
15.1 Cumplimiento de los requisitos legales.
15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.
15.3 Consideraciones sobre las auditorías de los sistemas de información.
15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sistemas de información.

2.2.3 Desarrollo de controles particulares

La norma es una recopilación de las mejores recomendaciones en la práctica de la seguridad de la información, sin embargo de ser requerida la implementación de un control no incluido, la norma lo permite, ya que no todos los controles y lineamientos son aplicables para todas las organizaciones. El desarrollo y adopción de un nuevo control, debe ser adecuadamente documentado de forma que facilite una futura revisión y comprensión por parte de los auditores, directivos, miembros y socios comerciales de la organización.

Tomando en cuenta, el tamaño de las empresas a las cuales se dirige el presente estudio, no se pretende que inviertan en la obtención de una certificación internacional ISO 27001, que representa una inversión económica considerable, sino que se pretende desarrollar una guía para que incluyan las mejores prácticas recomendadas por la norma NTE INEN ISO/IEC 27002 y que sean aplicables a su realidad.

CAPÍTULO III

Levantamiento de Activos de la Información

En el presente capítulo se analizará la red de datos de la oficina matriz de ACOTECNIC Cía. Ltda., ubicada en la ciudad de Cuenca en la Autopista Cuenca - Azogues y Pueblo Aguarura Km 17.1 sector Challuabamba; mediante un levantamiento de sus activos de información, categorizados en ocho grupos: hardware, software, comunicaciones, servicios de red, red, información, personas y procesos.

1. Presentación de la Compañía [19]

"ACOTECNIC Cía. Ltda. Asociación de Consultores Técnicos es una de las principales firmas de Consultoría en el campo de la Ingeniería del Ecuador, desde su fundación en el año 1994, realizada en la ciudad de Cuenca, ha colaborado en importantes proyectos tanto para entidades públicas (organismos internacionales, gobiernos regionales, ministerios, etc.) como para empresas privadas.

La organización que mantiene la empresa se basa en la premisa de poner al servicio de sus clientes una organización de alto nivel, autosuficiente, dotada de todos los recursos físicos que pudieran ser necesarios para tener un control permanente en la ejecución de los servicios que oferta.

ACOTECNIC ha evolucionado, desde una compañía consultora dedicada a la ingeniería sanitaria a una compañía diversificada con amplias capacidades en varias disciplinas. Actualmente la Compañía ofrece una oferta integrada de servicios que abarca desde evaluaciones preliminares hasta la puesta en marcha de pequeños y grandes proyectos"

[19] Fuente: www.acotecnic.com

Misión:

"Ofrecer Servicios de Asesoría y Consultoría de alta calidad y especialización en el diseño, fiscalización y gerenciamiento de Proyectos de Ingeniería Civil e Ingeniería Ambiental buscando continuamente satisfacer las necesidades de nuestros clientes así como mejorar la calidad de vida de nuestros colaboradores y mantenernos al día con las tecnologías más adecuadas, todo esto a través de nuestra política de calidad organizacional."

Visión:

"En el 2014 ACOTECNIC CÍA. LTDA. Será una organización sólida y sostenible operando proyectos nacionales e internacionales y con un modelo de gestión que apoye continuamente al desarrollo de la Empresa."

Valores Institucionales:
- Confianza.
- Confidencialidad.
- Comunicación.
- Trabajo en Equipo.
- Ética Profesional.
- Compromiso con los principios organizacionales.

2. Levantamiento de Activos de Información.

La seguridad informática tiene como objetivo proteger la información que la entidad posee dentro de los activos tales como: servidores, switches, etc., tomando en cuenta propiedades como: confidencialidad, disponibilidad e integridad.

A continuación se presenta el levantamiento de los activos de información dentro de ACOTECNIC, lo cual nos dará una idea clara del funcionamiento de la Compañía con respecto a la parte informática; para lograr establecer las políticas de seguridad necesarias.

2.1 Hardware

Se especifica todo el hardware: computadoras portátiles, de escritorio, impresoras, escáner, plotter; del que se dispone en la oficina principal para llevar a cabo sus diversos procesos. En esta tabla se muestran las diferentes categorías de ubicación para los activos de hardware:

COMPUTADORAS		
Área Administrativa u Operativa	**N° Activos**	**Activo**
Gerencia	2	Equipo 12
		Equipo 13
Presidencia	2	Equipo 2
		Equipo 14
Financiero Talento Humano	2	Equipo 4
		Equipo 8
Coordinación de Calidad	1	Equipo 8
Contabilidad	2	Equipo 4
		Equipo 5
Secretaría	1	Equipo 3
Preparación de Ofertas	1	Equipo 6
Programación y Control de Proyectos	1	Equipo 8
Sistemas	5	3 Equipo 4
		Equipo 11
		Equipo 15
Biología	2	Equipo 6
		Equipo 7
GIS	2	2 Equipo 8
Técnico	8	Equipo 3
		Equipo 4
		Equipo 5
		Equipo 6
		3 Equipo 8
		Equipo 10
No asignado	5	Equipo 1
		Equipo 3
		Equipo 5
		Equipo 8
		Equipo 9

Tabla 3.1: Activos - Computadoras

IMPRESORAS, PLOTER		
Área Administrativa u Operativa	**N° Activos**	**Activo**
Financiero Talento Humano	1	Epson Stylus TX420W
Secretaría	1	HP LaserJet Pro 400 Color
Preparación de Ofertas	1	HP Color LaserJet CP3525N
Técnico	1	HP Color LaserJet CP3525DN
Área de Impresión y Ploteo (Impresoras de Red)	5	Xerox Phaser 7400
		HP Color LaserJet 5550DN
		Xerox WorkCentre 4600
		Plóter HP Designjet 500
		Plóter HP Designjet T610

Tabla 3.2: Activos– Impresoras, Plotters

El equipamiento informático del cual dispone la Compañía está actualizado y en general con buenas características para el desarrollo de los diferentes procesos. Existe cierto número de computadoras obsoletas pero no se las ha inventariado puesto que van a ser donadas a escuelas públicas.

Para un detalle de las especificaciones técnicas de los activos de hardware consultar el anexo de hardware. [20]

2.2 Software

Se muestran los programas de los que está provista la Compañía, especialmente aquellos que están destinados a almacenar datos.
Antes de asignar una máquina a un colaborador, pasa por el Departamento de Sistemas y es allí en donde se instalan los programas básicos y los especializados para cada actividad.

Los programas básicos instalados son:

[20] Referirse a la sección de Anexos en la página 162

SOFTWARE BÁSICO	
Sistema Operativo	Windows 7 Ultimate
Antivirus	Eset Smart Security 2014 – 2015
Manejo de Archivos	Office Standard 2013 SNGL OLP NL
	Adobe Reader XI versión 11.0.10 - Español
	Nitro PDF Professional v6.0.1.8
Reproducción Multimedia	Adobe Flash Player 16 NPAPI
Grabar Archivos	CD Burner XP
Visor de Imágenes	Picasa v3.9
Compresor de Archivos	7 – Zip v9.20
Navegación en Internet	Internet Explorer v10.0.92
	Google Chrome
	Mozilla Firefox v29.0.01
Comunicación	Spark v2.6.3.12555
	Skype v7.3.0.101
Mantenimiento	CCleaner v3.11.1541
	Total Commander v8.0B11
	Team Viewer v8.0.30992

Tabla 3.3: Activos de Software

A continuación un listado de las aplicaciones especializadas

SOFTWARE ESPECIALIZADO	
Area Administrativa u Operativa	**Aplicación**
Financiero Talento Humano	Software Contable
	DIMM Formularios
Contabilidad	Software Contable
	DIMM Formularios
Programación y Control de Proyecto	Project 2013 SNGL OLP NL PROFESSIONAL
	Interpro
Sistemas	Windows Server 2012 SNGL OLP NL USERCAL
	Linux Debian
	Lion 10.6.8
Biología	Map Source
GIS	ArcGIS for Desktop basic simple use primary maintenance 2014 - 2015
	Autodesk Autocad 2014
	ENVI
	Map Source
Técnico	Autodesk Autocad 2014

Tabla 3.4: Activos de Software Especializado

En general cada máquina cuenta con el software apropiado para desarrollar las actividades de cada empleado. Sin embargo no está controlada la instalación de programas extras.

El firewall usado en todos los equipos es el que trae por defecto el Sistema Operativo Windows.

2.3 Comunicaciones

A continuación se van a detallar los distintos tipos de comunicaciones de los que dispone la Compañía y la red de datos, incluyendo activos como: switch, fax, teléfonos, módems.

COMUNICACIONES		
No. Activos	**Nombre**	**Propiedad**
15	Teléfonos Fijos	De toda la Compañía
1	Faxes	De toda la Compañía
1	Switch 48 puertos	De toda la Compañía
1	Switch 24 puertos	De toda la Compañía
1	Access Point	De toda la Compañía
1	Módem (Etapa)	ISP
1	Centralilla de 24 línea con 3 de entrada	De toda la Compañía

Tabla 3.5: Activos de Comunicaciones

La mayoría de los equipos de comunicaciones, se encuentran en buen estado y funcionamiento, la mayoría son nuevos puesto que la Compañía cuenta con una oficina propia desde hace poco más de tres años.

2.4 Servicios de red

Por lo general los servicios de red están instalados en uno o más servidores para proporcionar recursos compartidos a clientes-computadoras.
A continuación se describirá la estructura de red con la que cuenta la Compañía

2.4.1 Servidor Proxy y de Antivirus

ACOTECNIC dispone de un servidor HP de virtualización en donde corren:

1. Una máquina virtual con Linux Debian en donde se administra la red; está además, el servicio proxy cuya función es registrar el uso de internet, administrar el acceso de los sitios web restringiendo aquellas páginas consideradas dañinas e inadecuadas para el ambiente laboral. Es decir, el proxy actúa como un intermediario entre los usuarios y la Internet.
2. Una máquina virtual Windows Server en donde está el servidor de antivirus.

Los servicios DNS (Domain Name System) DHCP (Dynamic Host Configuration Protocol) están a cargo del servidor Debian.

2.4.2 Servidor Web almacena los respaldos de contabilidad en un hosting en Estados Unidos.

2.4.3 Servidor de Correo se almacena en un hosting en Estados Unidos.

2.4.4 Servidor BSCW Basic Support for Cooperative Work, es la plataforma de gestión de tareas de los diferentes proyectos. Reside en un hosting en Alemania.

Existe una máquina potente en la cual se respalda la información.

El servicio de hosting es compartido[21]; se debe considerar que en este tipo de servicio es el proveedor el que se tienen que encargar de mantener los sistemas, de hacer copias de seguridad, de atender tus consultas, etc.

[21] El hosting compartido es el servicio más básico, el más económico, el más fácil de usar y el utilizado en la mayoría de casos.

En el Departamento Financiero se maneja una base de datos, que es respaldada en el servidor web.

En la tabla 3.6 se muestran las diferentes categorías de ubicación para los servicios de red:

SERVICIOS DE RED		
No. Activos	**Nombre**	**Propiedad**
1	DNS	De toda la compañía
1	DHCP	
1	Correo	
1	Web	
1	Gestión Tareas	Proyectos
1	Base de Datos	Financiero
1	Proxy	De toda la compañía
1	Antivirus	

Tabla 3.6: Activos de Servicios de Red

2.5 Red

2.5.1 Extranet

Está formada por un módem ADSL, para la salida al Internet de banda ancha a través del ISP de la Empresa ETAPA EP (Empresa Pública Municipal de Telecomunicaciones, Agua Potable, Alcantarillado y Saneamiento); al cuál se conecta el servidor de virtualización. Dentro de éste se encuentra el servidor proxy que es el encargado de permitir el acceso a Internet de todos los equipos de la organización de forma indirecta a través de él.

Al ISP se conecta también, el servidor de correo que está en un hosting en Estados Unidos, el servidor web en donde se respalda la información de contabilidad en un segundo hosting en Estados Unidos. La página web de la compañía www.acotecnic.com está en este servidor.

Además se conecta con un servidor en Alemania para en donde se almacena la plataforma BSCW [22] para la gestión de tareas.

[22] Plataforma de Gestión de Tareas BSCW Basic Support for Cooperative Work

Un switch de 48 puertos con un Access Point configurado como enrutador, permiten la conexión al wireless de la Compañía.

2.5.2 Intranet:

Se establece a partir del switch de 48 puertos mencionado en la sección anterior, sobre el cual se enlazan las impresoras, uno de los plotters, además de las computadoras de escritorio.

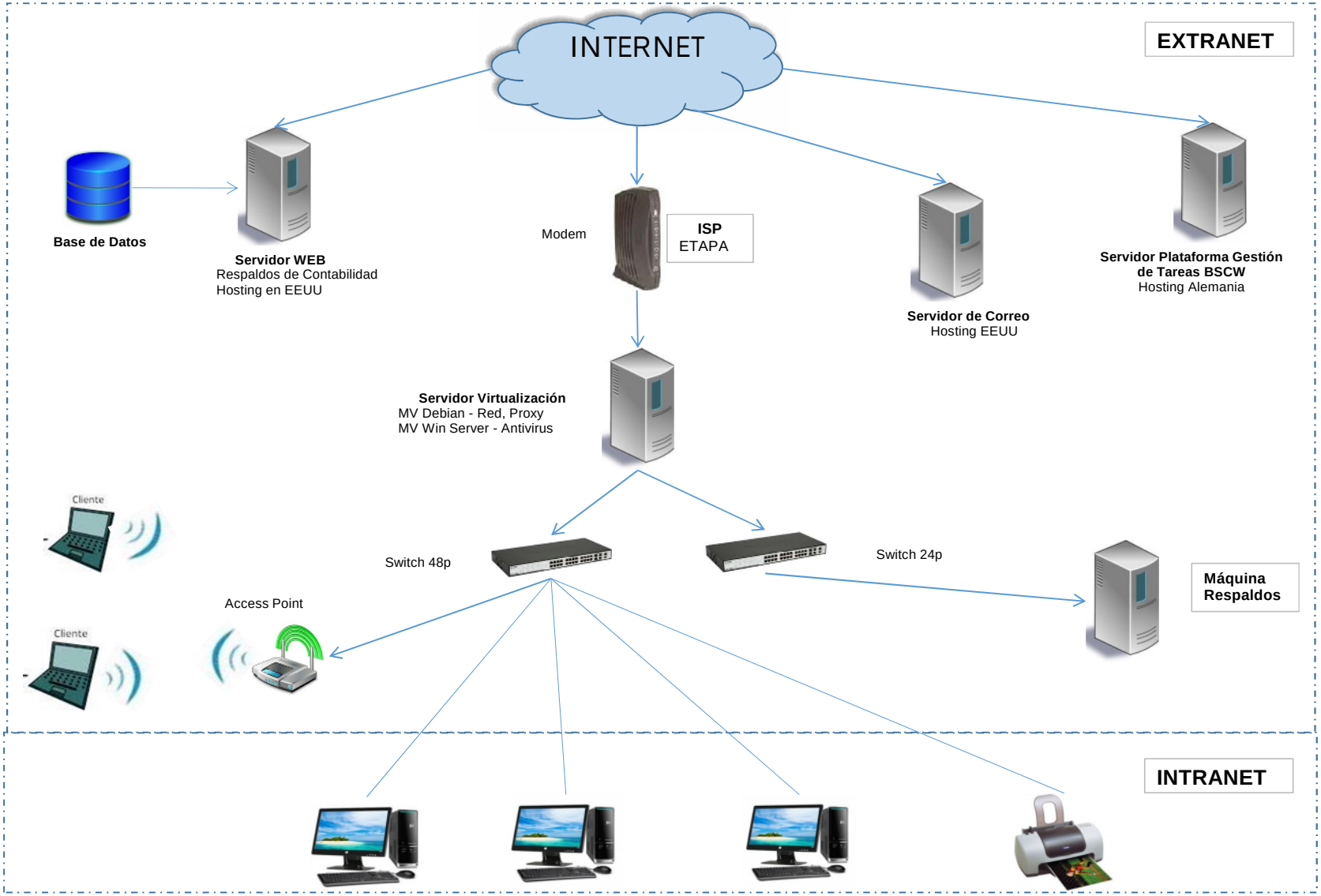
2.5.3 Topología de Red

La topología utilizada es la conexión en árbol, la cual posee un nodo de enlace troncal, ocupado por el switch de 48 puertos, desde el que se ramifican los demás nodos, para que pasen todos los paquetes de datos e información hacia toda la red.

Si se ocasiona una falla en un nodo no implicaría interrupción en las comunicaciones; a pesar de compartir el mismo canal de comunicaciones; simplemente el nodo queda aislado.

En la figura 3.1 se presenta el esquema actual de la red:

Figura 3.1: Esquema de red



2.6 Información como activo de ACOTECNIC

Se determina los tipos de información que se maneja dentro de la Compañía, pudiendo clasificarla en pública y privada.

2.6.1 Política de manejo de información pública

La denominamos “pública” ya que está disponible para gente que no labora en la oficina, sin embargo la información generada por ACOTECNIC no es accesible para todo tipo de usuario. Son aquellos archivos, registros o datos, resultado de los estudios realizados que son entregados a cada cliente, y con autorización de ellos, se podría entregar una copia, previo una solicitud escrita. La información generada está disponible para el equipo de trabajo de cada proyecto.

Existen datos como la misión, visión, política de calidad y demás información de este tipo que está disponible para todos los miembros de la Compañía.

2.6.2 Política de manejo de información privada

Son aquellos datos que son confidenciales. Es inviolable, por ende su lectura, modificación o cualquier tipo de manipulación por parte de personas ajenas a ella, está prohibida. La información considerada como privada dentro de la Compañía es: nómina de clientes (empresas contratantes), nómina de proveedores (especialista para la ejecución de los proyectos), archivos del área de Contabilidad, etc.

En la siguiente tabla se señalan los diferentes tipos de información de la Compañía:

INFORMACIÓN		
Propiedad:	**Nombre del Activo**	**Tipo de Información**
Gerencia	Toda la información existente en la Compañía	Pública y Privada
Presidencia	Toda la información existente en la Compañía	Pública y Privada
Financiero, Contabilidad	Estado financiero y contable de la Compañía, contratos con clientes y proveedores, roles de pagos del personal, Pólizas, etc.	Privada
Talento Humano	Datos del personal	Privada
Coordinación de Calidad	Manejo del programa de gestión de calidad de la Compañía, Indicadores, No conformidades, Resultados de auditorías externas e internas.	Privada
Secretaría, Proveeduría	Oficios, registros de proveeduría	Privada
Preparación de Ofertas	Nómina de clientes y proveedores, Ofertas técnicas y económicas.	Privada
Programación y Control de Proyectos	Cronogramas de proyectos, Control de Planillas de los proyectos.	Privada
Mantenimiento	Estado de los equipos, vehículos.	Privada
Sistemas	Accesos a servidores, equipos, correos. Inventario de equipos.	Privada
Biología, GIS, Técnicos	Información entregada por clientes para los proyectos, información generada en los estudios.	Pública

Tabla 3.7: Activos de Información

Al iniciar un proyecto se hace entrega de toda la información base[23] recibida de los clientes o generada por ACOTECNIC, sin embargo no siempre la resguardan adecuadamente, haciéndose en varios casos copias a terceros o pérdidas de los archivos.

Al terminar los proyectos no existe un proceso definido para respaldar la información, documentos finales quedan en las computadoras de los técnicos o personal que fue contratado para cierto proyecto, en ocasiones se pierden las versiones finales de ciertos archivos.

[23] Información Base: Documentos, archivos de estudios previos, libros, cartografía existente al iniciar un estudio.

Conversaciones confidenciales son tratadas en ambientes abiertos. En muchas ocasiones el acceso a información de los servidores se la realiza sin mayor control.

2.7 Personas

Dentro de la Compañía se distinguen los siguientes grupos en cuanto a personal de planta: dirección general, personal administrativo, personal técnico, personal de apoyo.

Para cada proyecto, se contrata un director y subdirector de proyecto, una secretaria, especialistas en las diferentes áreas del estudio, un chofer; (el personal contratado dependerá del tipo de proyecto, monto y tiempo en el que se desarrollará).

Para la selección y ubicación de los cargos se toman en cuenta características como: conocimientos, experiencias, motivación, intereses vocacionales, aptitudes, actitudes, habilidades, potencialidades, salud, etc.

A continuación se indican los diferentes tipos de activos de personas de los que dispone la compañía, considerando su cargo, función y jerarquía.

PERSONAL		
N° Activos	**Propiedad**	**Tipo Persona**
1	Gerencia	Dirección General
1	Presidencia	
1	Coordinación de Calidad	Administrativo
1	Financiero Talento Humano	
2	Contabilidad	
1	Secretaría	
1	Preparación de Ofertas	Técnico
1	Programación y Control de Proyectos	
1	Mantenimiento	
1	Sistemas	
2	Biología	
1	GIS	
3	Técnico	
1	Mensajero	Personal de Apoyo
1	Chofer	
1	Limpieza	

Tabla 3.8: Activos de Personal

La nómina de empleados dentro de ACOTECNIC; consta de veinte personas. El organigrama general de la organización está claramente definido, y la asignación de cargos de forma jerárquica y ordenada.

2.8 Procesos

Un proceso es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico. [24]

A partir de una o varias entradas de información o productos, dan lugar a salidas de productos o información con un valor añadido.

ACOTECNIC Cía. Ltda. Emplea este conjunto de actividades sistematizadas para el cumplimiento del objetivo de su negocio que es la prestación de servicios. El cliente plantea sus requisitos, que se convierten en el objetivo del contrato; la

[24] Fuente: http://definicion.mx/proceso/#ixzz3XRS4S0iH, Fecha de ingreso: Marzo 2015

Compañía realiza el Diseño, Fiscalización, Asesoramiento, Gerenciamiento, Auditoría o Estudio y entrega los resultados al cliente. Esto se muestra en la figura 3.2:

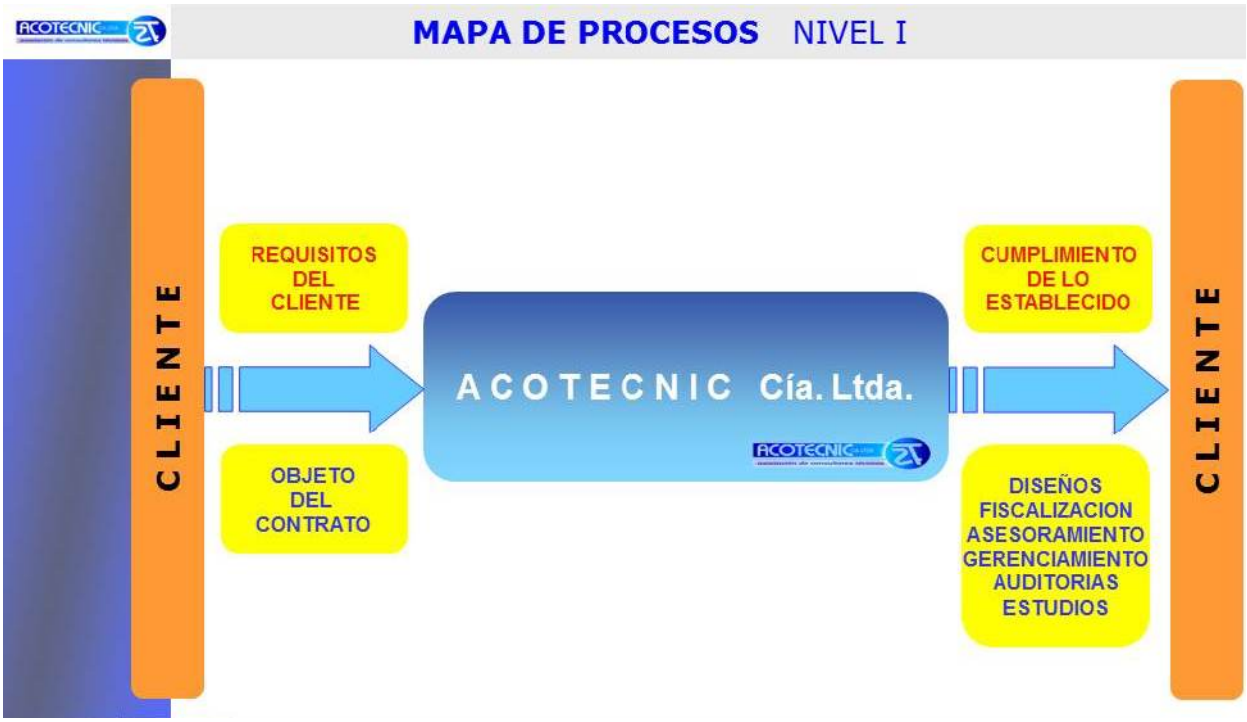


Figura 3.2: Mapa de Procesos Nivel I [25]

Los procesos dentro de la Compañía están correctamente definidos y ejecutados; ACOTECNIC cuenta con un sistema de calidad ISO 9001 con una Certificación IQ Net Management System.

Existen nueve procesos divididos en tres grandes grupos:

1. Estratégicos

Dentro de éste están los procesos: Gerencial, Gestión de Calidad y Auditorías Internas y Atención al Cliente.

[25] Fuente: www.acotecnic.com

2. Operativos

A esta categoría pertenecen los procesos de Preparación de Ofertas y Prestación de Servicios.

3.- Apoyo

Aquí están los procesos de Recursos Humanos, Proveeduría, Mantenimiento y Metrología y Sistemas.

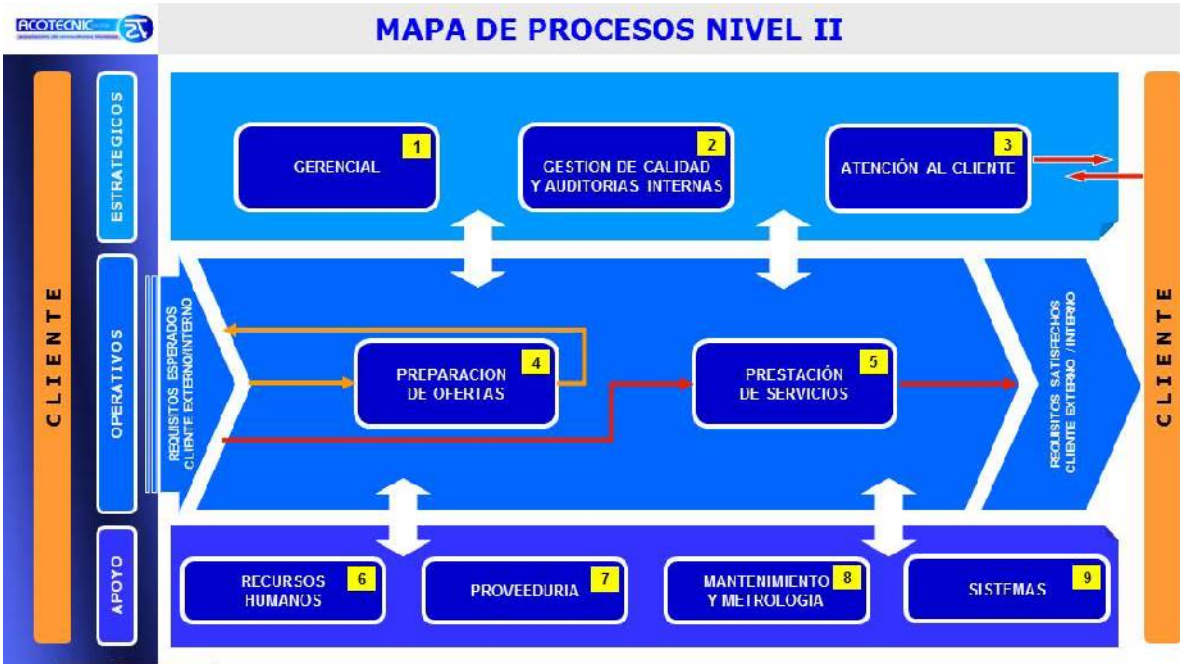


Figura 3.3: Mapa de Procesos Nivel II [26]

En esta tabla se muestran las diferentes categorías de ubicación para los procesos:

[26] Fuente: www.acotecnic.com

PROCESOS			
No. Activos	Nombre Activo	Propiedad	Tipo
1	Gerencial	Gerente, Presidente	Proceso
1	Gestión de Calidad y Auditorías Internas	Coordinación de Calidad	Proceso
1	Atención al Cliente	Secretaría, Financiero.	Proceso
1	Preparación de Ofertas	Preparación de Ofertas, Presidencia	Proceso
1	Prestación de Servicios	Director Proyecto, Técnico, Mensajero, Chofer	Proceso
1	Recursos Humanos	Talento Humano	Proceso
1	Proveeduría	Secretaría, Proveeduría	Proceso
1	Mantenimiento y Metrología	Mantenimiento	Proceso
1	Sistemas	Sistemas	Proceso

Tabla 3.9: Activos de Procesos

CAPÍTULO IV

Identificación de riesgos de ACOTECNIC basados en las recomendaciones dadas por la norma ISO/IEC 27002.

El presente capítulo se apoya en la traducción al español de la norma ISO/IEC 27002, versión peruana, que está disponible en internet bajo el nombre “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información” 2a. Edición.

Se hace una revisión de la norma ISO/IEC 27002, evaluando los controles que sean aplicables a la situación actual de la Compañía y se estima el porcentaje de cumplimiento de cada uno. Para cuantificar estos valores se hace una comparación, entre los controles recomendados en la guía de implementación, los datos obtenidos en las visitas de campo, en las entrevistas con personal de la compañía e información disponible en la página web de la Compañía.

Aplicando técnicas para calcular índices de gestión, se introduce en el análisis, una variable de carácter cualitativo, que es la importancia que tiene cada control dentro de los procedimientos de la Compañía.

1 Política de seguridad

1.1 Documento de política de seguridad de la información

La Compañía no dispone de un documento específico, relacionado con Políticas de Seguridad de la Información, sin embargo existen algunas disposiciones dadas por parte de Gerencia con el objetivo de regular el uso de los activos, especialmente los recursos de red.

Las disposiciones están dirigidas al personal de planta y son comunicadas mediante memos, en los cuales se detallan la disposición y las sanciones a aplicarse en caso de no acatar dichas instrucciones.

Estos comunicados surgen como una medida correctiva ante algún incidente de la seguridad de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

1.2 Revisión y evaluación.

Eventualmente la Gerencia toma medidas complementarias que sirven para reforzar o modificar las disposiciones al suscitarse algún incidente de la seguridad de la información; como una mejora en los procedimientos internos. Esta revisión, surge como una medida correctiva.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

2 Aspectos organizativos para la seguridad.

2.1 Organización interna

2.1.1 Compromiso de la Dirección con la seguridad de la información.

Por parte de Gerencia y de Presidencia se ha considerado la conveniencia de iniciar un proceso para mejorar el manejo de los activos de información de la Compañía.

Se han mantenido las primeras reuniones conjuntamente con un equipo de trabajo y se han definido algunos requisitos y necesidades para la organización de la seguridad de la información, puesto que ya se han suscitado incidentes relacionados con la pérdida de información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%, ya que existe el interés de parte de los Administradores en mejorar la seguridad de sus activos.

2.1.2 Coordinación de la seguridad de la información

Para la organización de la información de los proyectos ejecutados por la Compañía, se establecieron distintos roles para el grupo de trabajo.

El personal de TI [27] fue el encargado de recopilar los resultados de los distintos proyectos desarrollados, además de examinar todo el hardware y software necesarios para esta tarea. El Departamento de Programación y Control de Proyectos, fue el encargado de recopilar toda la información de las planillas [28] de proyectos; y, el Departamento de Coordinación de Calidad fue asignado para dar seguimiento a todos los avances.

Esta organización y distribución de trabajos fue de carácter eventual, y el objetivo fue realizar un inventario dentro de la Política de Gestión de Calidad de la Compañía.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%, ya que de alguna manera, cada equipo de trabajo

[27] Tecnologías de la Información: Amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información. Fuente: DICCIONARIO DE INFORMATICA Y TECNOLOGÍA disponible en http://www.alegsa.com.ar/Dic/tecnologias%20de%20la%20informacion.php

[28] Documentos en donde constan los volúmenes de obra ejecutados y facturados. Fuente: Procedimientos internos de ACOTECNIC

responde a una coordinación interna; sin embargo, no está enfocada directamente a la seguridad de la información.

2.1.3 Asignación de responsabilidades sobre seguridad de la información

La responsabilidad se encuentra centrada en el departamento de TI, que es quién realiza la tareas de monitoreo, detección de problemas, amenazas y vulnerabilidades; tomar acciones correctivas e informar a la Administración acerca de los problemas y novedades existentes en los activos de red y servicios asociados.

La Administración es la responsable de tomar la decisión final en cada caso. Generalmente es una acción correctiva.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%, ya que la responsabilidad debe ser tomada por todos y cada uno de las personas involucradas en las actividades de la Compañía, ya sea personal interno, proveedores externos, terceros o clientes. Al momento, la responsabilidad sólo está centrada en el manejo de los activos de red y los servicios asociados.

2.1.4 Proceso de autorización de recursos para el tratamiento de la información.

El departamento de TI mantiene un registro de equipos de la Compañía asignados a cada funcionario. Continuamente están ingresando proveedores externos, especialistas con su personal, cuyos equipos no están registrados.

Para facilitar la ejecución de las tareas, se les permite el acceso a la red de datos, esto pone en riesgo la integridad de la red interna y los activos de información.

Mediante el servidor se intenta bloquear el acceso a ciertas páginas de Internet como: música, entretenimiento, videos de youtube, sitios con contenido sexual; para reducir los posibles ataques de virus. Sin embargo algunos funcionarios cuentan con determinados privilegios, autorizados por Gerencia, y no tienen dichas restricciones, convirtiéndose en vulnerabilidades para la seguridad de la información.

Existe un uso inadecuado de Internet por parte del personal de planta y externo, lo que provoca que se sature el ancho de banda con mucha frecuencia. Esto ha ocasionado llamados de atención por parte de Presidencia al responsable del Departamento de Sistemas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%, ya que no está definido un procedimiento. De alguna forma se trata de mantener este control, sin embargo se brindan privilegios a determinados usuarios por pedido de los Gerentes de Proyecto y aprobación de parte de los Administradores, sin considerar el impacto que esto tendrá en la operación de la red y sus servicios.

2.1.5 Acuerdos de confidencialidad

Desde el momento que un proyecto es adjudicado, se empieza a enviar información entregada por el cliente o propia de ACOTECNIC; a los especialistas, proveedores externos o su personal de trabajo. No existe acuerdo explícito de confidencialidad, no divulgación y buen uso, sobre los recursos que les son entregados.

En ocasiones, algunos proveedores externos han solicitado se les vuelva a entregar la información porque se les ha extraviado.

Tampoco existen estos acuerdos de forma explícita al interior de la Compañía.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

2.1.6 Contacto con las autoridades

No están especificados los procedimientos, canales a utilizarse en caso de un evento o a qué autoridad acudir en caso de presentarse un incidente. Cuando se presenta un problema, el responsable del Departamento de Sistemas realiza los contactos necesarios con el fin de solucionar el problema. Una vez corregido el incidente todo vuelve a su ritmo normal.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

2.1.7 Contacto con grupos de interés especial

No aplica este control a la Compañía.

Para el análisis de la situación actual de la Compañía no se considera que este control.

2.1.8 Revisión independiente de la seguridad de la información

Al no existir una política de seguridad establecida, no están definidos los objetivos, controles, procesos ni procedimientos relacionados con la seguridad de la información. Sin embargo, existe el interés de parte de la Administración de la Compañía en conocer el estado de la seguridad de la información, por lo que han aceptado formar parte de esta investigación, constituyéndose una primera revisión independiente dentro de ACOTECNIC Cía. Ltda.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

2.2 Seguridad en los accesos de terceras partes

2.2.1 Identificación de riesgos por el acceso de terceros

No se cuenta con políticas específicas acerca del acceso de proveedores externos a los activos. En muchas ocasiones solicitan información en reiteradas ocasiones, sin documentar los nuevos pedidos. Entre las causas más comunes, expuestas para justificar dichos pedidos están daño en la información y/o pérdida.

La entrega inicial de información se realiza mediante oficio, sin embargo en las futuras entregas se notifica por correo, pero no se deja de manifiesto acuerdos de confidencialidad, no divulgación o buen uso de la información.

La pérdida de información constituye una amenaza que puede poner en riesgo la continuidad del negocio, deterioro de relaciones comerciales, pérdida de una ventaja competitiva y retrasos en la ejecución de actividades, que podrían culminar en sanciones económicas por retardos en los cronogramas de ejecución.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

2.2.2 Requisitos de seguridad cuando sea trata con clientes

El intercambio de información se realiza mediante oficios, para evidenciar los tiempos de ejecución de los contratos y para cumplir los procedimientos de la política de gestión de calidad. Sin embargo este intercambio de información no garantiza la confidencialidad, la integridad y la autenticidad de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

2.2.3 Requisitos de seguridad en contratos de out sourcing

El intercambio de información entre la Compañía y los proveedores externos, se da por medio de oficios y actas de entrega recepción. No está designada una persona por el proveedor externo, para que sea la responsable de la recepción, custodia y transporte de la información; lo que podría provocar pérdida y fuga de información.

Para facilitar las labores de los proveedores, se permite el acceso a determinados activos, especialmente la red de datos, esto constituye un riesgo ya que al ser equipos que no están dentro del inventario de la Compañía, difícilmente se podría hacer un seguimiento y determinar responsabilidades en caso de presentarse algún incidente.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

3 Gestión de activos

3.1 Responsabilidad por los activos

3.1.1 Inventario de los activos

El hardware de la Compañía está siendo actualizado y revisado continuamente. La existencia de equipos obsoletos, dañados o dados de baja dificulta el manejo de este inventario, puesto que no se define un procedimiento a seguir con estos equipos y permanecen en la bodega de la Compañía.

Los inventarios de comunicaciones, servicios de red, equipos de red fueron levantados una sola vez, hace aproximadamente tres años, cuando se implementaron las redes en la nueva oficina matriz.

El inventario de procesos está claramente definido, es el que mejor se maneja en la Compañía. La certificación de calidad que ésta posee, así lo exige.

En cuanto al software, la Compañía mantiene un inventario de los programas utilitarios y especializados con sus respectivas licencias para el desarrollo de su actividad. Sin embargo, cada usuario tiene la libertad de instalar en su equipo asignado el software que estime necesario para facilitar sus actividades.

Esto constituye una gran vulnerabilidad debido a que los mismos son descargados mediante internet desde sitios no seguros, introduciendo en sus equipos y posteriormente a la red de datos: virus, gusanos, programas maliciosos, troyanos, etc., que afectan el desempeño y comprometen la seguridad de los activos de información.

El inventario de información no está adecuada ni claramente definido. Muchas veces no se cuenta con la última versión de la información de los estudios realizados en proyectos anteriores.

No se cuenta con un proceso claro para respaldar la información; no se respalda a tiempo o se respalda todo el contenido de un computador sin saber exactamente qué tipo de información existe. En ocasiones se encuentra en los respaldos varias versiones de un mismo proyecto e incluso información personal de los empleados.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

3.1.2 Propiedad de los activos

Los activos de hardware, software, comunicaciones y red, están a cargo del responsable del Departamento de Sistemas; sin embargo no se cuenta con documentación acerca de la estructura de la red, la configuración de los servidores, claves de acceso a equipos.

La política de calidad de la Compañía, exige la documentación de soporte de la transferencia de equipos, responsabilidad de su uso, claves para manejo de licencias de software.

Los activos de personal son manejados por el Departamento de Talento Humano y, la información de clientes y proveedores, está a cargo del Departamento de Preparación de Ofertas.

La propiedad, custodia y responsabilidad de los activos de información resultantes de estudios y proyectos realizados no está definida.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

3.1.3 Uso adecuado de los activos

Algunos recursos como el acceso a internet, son manejados inadecuadamente; debido a la utilización de este activo para actividades personales o de entretenimiento; ocasionando retrasos en las actividades de trabajo, ya que este recurso es limitado.

No existen políticas definidas con proveedores, especialistas externos para el uso, confidencialidad y no divulgación de la información. Se tiene conocimiento que en varias ocasiones, la información se ha extraviado, o la entregan a terceros sin ninguna restricción y sin saber el uso que le van a dar a este activo de la Compañía.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

3.2 Clasificación de la información

3.2.1 Lineamientos de clasificación

La Compañía cuenta con información restringida, especialmente la información contable y la información de estrategias comerciales. Sin embargo es necesario que se determine la importancia de la información operativa y la información resultante de los proyectos ejecutados, ya que esto podría comprometer la ventaja competitiva que la Compañía ha logrado alcanzar durante desarrollo de cada proyecto.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

3.2.2 Marcado y tratamiento de la información.

No están definidos procesos de identificación, etiquetado y tratamiento de la información. Los procesos actualmente utilizados para estas actividades se limitan al criterio de la propietario responsable de la información, pero no existe un formato o procedimiento unificado.

Toda la información de los equipos devueltos a la Compañía es almacenada en el servidor de respaldos sin ninguna restricción o clasificación.

Algunos departamentos disponen de unidades de almacenamiento portátiles como discos externos y memorias flash. Estos dispositivos no cuentan con ninguna protección adicional más que la custodia de su responsable.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

4 Seguridad en recursos humanos

4.1 Seguridad antes del empleo

4.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales.

No se cuenta con procedimientos definidos que permitan determinar si los candidatos son los más idóneos respecto al cuidado y protección de la información. La selección de personal básicamente se centra en la capacidad técnica y experiencia de los candidatos.

Durante las entrevistas de selección no se establecen los compromisos de confidencialidad, no divulgación y buen uso de la información a la cual pudieran tener acceso, incluyendo documentos, archivos, acceso a instalaciones, etc.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

4.1.2 Investigación de referencias y selección de personal

Una vez seleccionados los candidatos, se realiza una validación de la información registrada en las hojas de vida, en lo referente a experiencia laboral y capacidad técnica. No se solicitan referencias sobre su experiencia en el cuidado y manejo de activos de información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

4.1.3 Acuerdos de confidencialidad

Una vez culminada la etapa de selección, las relaciones laborales se concretan mediante la firma de un contrato de trabajo con el candidato elegido. No se incluyen dentro de este proceso de contratación, la aceptación y el compromiso para mantener la seguridad de la información, compromisos de no divulgación, de confidencialidad y de buen uso de los recursos que se le asignen.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

4.2 Durante el empleo

4.2.1 Responsabilidades de la Gerencia

Los Administradores de la Compañía son los responsables de dar las instrucciones para la ejecución de los trabajos, las mismas que están orientadas en su mayoría al desarrollo de actividades y al cumplimiento de la política de gestión de calidad.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

4.2.2 Conocimiento, educación y capacitación en seguridad de la información

La Compañía durante sus años de trabajo, ha venido elaborando varios documentos que son utilizados para la capacitación interna del personal, especialmente lo relacionado al cumplimiento de la política de gestión de calidad, uso de correo electrónico, uso de activos, rutas de evacuación.

Sin embargo, no existe un programa de capacitación para la seguridad de la información. Constituyéndose una amenaza latente, ya que la mayor cantidad de riesgos para la seguridad de la información se atribuyen al factor humano.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

4.2.3 Proceso disciplinario

No existe un proceso disciplinario definido para las infracciones a la seguridad de la información, no obstante se intenta disuadir a los empleados para que no hagan un mal uso de los recursos, mediante sanciones económicas o amonestaciones verbales.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

4.3 Finalización o cambio de empleo

4.3.1 Responsabilidades de finalización

No están definidas las responsabilidades acerca de la devolución, cambio y traspaso de los activos de la información, de empleados que finalizan su responsabilidad laboral o son asignados a nuevas actividades.
El personal no está consciente que los activos son de propiedad de la Compañía, incluyendo la información generada por el empleado durante la vigencia del contrato de trabajo.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

4.3.2 Devolución de los activos

Cuando un empleado termina su contrato, devuelve todos los activos de hardware asignados para sus actividades laborales.

No se tiene un control sobre la devolución de información en físico o en digital, y si se realizaron copias de información en unidades de almacenamiento de propiedad del empleado, o si estás fueron eliminadas apropiadamente. Tampoco existen instrucciones claras acerca de la forma en que la información debe organizarse previa la devolución y/o transferencia.

Frecuentemente los activos devueltos tiene información repetida, archivos personales, videos, fotografías y más archivos que no son de utilidad para la Compañía; esto dificulta el uso de dichos recursos, ya que es necesario invertir tiempo en buscar y organizar la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

4.3.3 Retiro de los derechos de acceso

La Compañía maneja un correo corporativo, cuando un empleado termina su contrato, su cuenta es eliminada y reemplazada por una nueva.

El acceso a la plataforma de trabajo es eliminado una vez que se haya terminado la participación de un técnico dentro del proyecto.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

5 Seguridad física y ambiental

5.1 Áreas seguras

5.1.1 Perímetro de seguridad física

ACOTECNIC adquirió una edificación, la misma que ha sido adecuada para sus actividades comerciales. La edificación está monitoreada todo el día.

Existen sensores de movimiento en distintas oficinas. Se ha contratado los servicios de un guardia de seguridad para las noches. A pesar de esto, la Compañía ha sido víctima de la delincuencia y ya sufrió un robo de computadores, y varios intentos fallidos de ingreso al local por las noches.

La información operativa permanece en las oficinas, las cuales cuentan con una seguridad escasa. La información sensible se encuentra almacenada en servidores remotos.

La información física utilizada en las actividades diarias se guarda, con las respectivas seguridades, en los puestos de trabajo. Algunos departamentos no cuentan con puertas de ingreso, son salas compartidas con otros profesionales, a las que se puede acceder, sin restricción alguna, luego de pasar por la recepción.

La información de proyectos anteriores está guardada en la bodega de la Compañía con su respectiva seguridad para el ingreso.

Se cuenta con una recepcionista y un área de recepción para controlar el acceso a las oficinas.

Los servidores de la Compañía están ubicados en un cuarto independiente, al que sólo debería acceder personal autorizado. Se pudo verificar que no cuenta con las seguridades adecuadas, la chapa ha sido forzada en varias ocasiones.

En cuanto a la seguridad perimetral, una de las puertas de acceso a los parqueaderos se encuentra dañada, según indican, hace ya varios meses, lo que obliga a que se mantenga abierta durante la jornada de trabajo, constituyéndose en una vulnerabilidad a ser considerada prioritaria.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

5.1.2 Controles de ingreso físico

El ingreso por la puerta principal cuenta con un intercomunicador, con cámara de video. En ocasiones las personas que ingresan no tienen la precaución de cerrar la puerta luego de su ingreso. Lo que posibilita que otras personas puedan acceder a las instalaciones sin el conocimiento de la recepcionista.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

5.1.3 Asegurar las oficinas, habitaciones y medios

Al haber reutilizado una edificación existente, la distribución de oficinas se realizó en base a la disponibilidad de espacio. Los departamentos Administrativos cuentan con habitaciones separadas, con las respectivas seguridades, sin embargo algunos departamentos operativos comparten salas amplias y no cuentan con puertas de ingreso, o las mismas permanecen abiertas todo el tiempo.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

5.1.4 Protección contra amenazas externas e internas

En las instalaciones existen extintores, guías de evacuación en todas las oficinas señalando las posibles salidas de emergencia.

No hay extintores en sitios donde existen materiales de fácil combustión, por ejemplo la sala de ploteo, la bodega.

Las puertas consideradas como salidas de emergencia no brindan las condiciones operativas necesarias, en ocasiones el pulsante que abre una de las puertas suele fallar, mientras que la otra puerta permanece abierta todo el tiempo.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

5.1.5 Trabajo en áreas aseguradas

No existe una identificación de áreas seguras.

Para el análisis de la situación actual de la Compañía no se considera que este control.

5.1.6 Áreas de acceso público, entrega y carga

No existe mayor cuidado cuando gente que entrega suministros a la Compañía; debido a que son procesos comunes, o son realizados por personas conocidas, existe cierta confianza y se les permite que ingresen y se dirijan solos hacia los lugares de descarga.

La entrega de suministros de oficina se realiza directamente en la recepción.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

5.2 Equipo de seguridad

5.2.1 Ubicación y protección del equipo

Los servidores se encuentran instalados en una habitación independiente, protegidos de la humedad y el calor, sin embargo no cuenta con una seguridad adecuada lo que permite el acceso de personal no autorizado.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

5.2.2 Servicios públicos de soporte

Todos los equipos de la Compañía poseen su UPS [29]. El servidor principal está dimensionado para suministrar energía de soporte por un periodo de una hora y treinta minutos.

[29] UPS: Uninterruptible Power Supply - Fuente de alimentación ininterrumpida

El suministro de energía eléctrica y servicios de telefonía son suministrados por las empresas públicas locales.

El servicio de internet utiliza ADSL [30] y el servicio de telefonía son suministrados por la Empresa ETAPA EP.

No se cuenta con una conexión alternativa con otro proveedor, y con otra tecnología de acceso; en caso de producirse un fallo en las redes del proveedor, ambos servicios quedaría inutilizados. Esta vulnerabilidad puede poner en riesgo las actividades de comercio electrónico de la Compañía.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

5.2.3 Seguridad del cableado

Se tiene estándares de cableado eléctrico y de datos. Actualmente se utiliza en la parte eléctrica el cable No12, para datos se utiliza el cable UTP categoría 6 con conectores RJ45.

La oficina se adecuó en una casa existente. El cableado para datos no es certificado y está en canaletas sobrepuestas por las paredes.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

5.2.4 Mantenimiento de equipo

[30] ADSL: Asymmetric Digital Subscriber Line – Tecnología que permite la transmisión de datos a través de pares de cobre de líneas telefónicas.

Existe una sola persona en el Departamento de Sistemas, y es el responsable del mantenimiento y correcta operación de todos los equipos y servicio de red al interior de la Compañía.

No se da un plan de mantenimiento preventivo adecuado, debido a la falta de personal en el Departamento de Sistemas y a que no se considera la paralización de estaciones de trabajo para su mantenimiento.

La mayor parte del mantenimiento es correctivo, cuando alguno de los equipos ya presenta algún inconveniente.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

5.2.5 Seguridad de los equipos fuera del local

Existe un control para el ingreso y egreso de equipos, pero no una normativa de cómo debe ser tratado el equipo fuera de la oficina.

La responsabilidad de los equipos que salen de la oficina la asume el Director del Proyecto que está utilizando esos recursos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

5.2.6 Seguridad de la eliminación o re-uso del equipo

Antes de ser re asignado un equipo, se lo formatea y se instalan los programas requeridos por el nuevo usuario, sin embargo no existe un procedimiento definido para eliminar completamente la información. Habitualmente, se le realiza un formateo rápido y se instalan los nuevos programas.

En el caso de dispositivos de almacenamiento portátiles, cuando se presenta algún daño, se intenta recuperar la información mediante herramientas de software. De no conseguirse la recuperación de la información o del dispositivo, éste es considerado no utilizable y es dado de baja.

No existe un procedimiento definido para la destrucción o la forma de deshacerse de los equipos dados de baja, los mismos que son almacenados en bodega hasta que la Administración tome una decisión al respecto.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

5.2.7 Retiro de propiedad

El retiro de la propiedad sobre algún activo, se realiza con autorización de la Gerencia. Esta autorización se da luego que se haya analizado el pedido y los justificativos de parte del responsable, del Director del Proyecto o del Departamento de Recursos Humanos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 80%.

6 Gestión de las comunicaciones y operaciones

6.1 Procedimientos y responsabilidades operacionales

6*.1.1 Procedimientos de operación documentados*

Existe un manual sobre el uso del correo de la Compañía y manuales referentes al cumplimiento de las políticas de Gestión de Calidad, pero no existen documentos respecto a la seguridad de la información.

La configuración de los equipos de red no está documentada, lo que genera una dependencia del responsable de la red.

La capacitación sobre algunos procedimientos que no están documentados, se realiza por medio de reuniones de trabajo inter personales.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

6.1.2 Gestión del cambio

No se cuentan con políticas internas para la gestión de cambios.

Antes de efectuar cualquier cambio se analizan las posibles dificultades que se presentarían al realizar el cambio, por ejemplo la inestabilidad de un software, la falta de instaladores para el resto de aplicaciones especializadas, requerimientos mínimos de hardware.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

6.1.3 Segregación de los deberes

La Compañía no cuenta con políticas de segregación.

Existe separación de actividades por áreas de estudio y departamentos de trabajos, manteniendo cada uno distintos privilegios para el acceso a la plataforma de gestión de tareas y bases de datos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

6.1.4 Separación de los medios de desarrollo, prueba y operación

Control

Los medios de desarrollo, prueba y operación deberían estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional.

ANÁLISIS: No es aplicable a la Compañía.

La Compañía utiliza para sus actividades software desarrollado.

Para el análisis de la situación actual de la Compañía no se considera que este control.

6.2 Gestión de la entrega del servicio de terceros

6.2.1 Entrega del servicio

No existen controles definidos respecto a la seguridad de la información en la entrega de servicios por parte de terceras personas, como el mantenimiento de equipos especializados, impresoras, plotters, equipos de topografía.

Los términos del servicio se refieren a la calidad, atención oportuna, consideraciones económicas, garantía técnica. Para seleccionar la alternativa más conveniente se solicita la cotización de al menos tres proveedores.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

6.2.2 Monitoreo y revisión de los servicios de terceros

Previo a solicitar la asistencia técnica se realiza una revisión al interior de la Compañía, con el fin de obtener los reportes generados por el equipo. Estos reportes son utilizados como referencia.

Una vez solicitada la asistencia técnica, el proveedor seleccionado se encarga de hacer la revisión, de entregar el diagnóstico y establecer las posibles soluciones. No existe ningún monitoreo al respecto, hasta la recepción definitiva del equipo en condiciones operativas.

No se tiene precaución de proteger, eliminar o evitar el acceso de terceros a las unidades de memoria interna de estos equipos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

6.2.3 Manejo de cambios en los servicios de terceros

No existen controles de este tipo en los que se considere la seguridad de la información. La selección o cambio de los proveedores se realiza en base a la mejor propuesta considerando la calidad, atención oportuna, costo de servicio y garantía técnica.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

6.3 Planeación y aceptación del sistema

6.3.1 Gestión de la capacidad

El responsable del Departamento de Sistemas continuamente está monitoreando el rendimiento de los servidores, los avisos del antivirus y la utilización de la conexión a internet. Estas actividades son registradas en informes que son comunicados a la Gerencia y Recursos Humanos semanalmente. Sin embargo, estos informes no son tomados en cuenta de forma oportuna como base para tomar una decisión, lo que dificulta aplicar medidas correctivas sin la autorización de los Administradores de la Compañía.

Muchas de las medidas que se toman para optimizar el rendimiento de servicios de red, son de carácter correctivo emergente, cuando se presenta un reclamo.

Esto ha llevado a realizar un análisis de la ampliación de la capacidad de los servicios y una optimización de los mismos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

6.3.2 Aceptación del sistema

La Administración en base a los reportes generados debe tomar las decisiones más conveniente acerca de la aceptación o mejora del sistema, viéndose muchas veces limitados por la situación económica de la Compañía.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

6.4 Protección contra el código malicioso y móvil [31]

Objetivo: *Proteger la integridad del software y la integración.*

6.4.1 Controles contra códigos maliciosos y 6.4.2 Controles contra códigos móviles

No existen controles definidos para la protección contra códigos maliciosos.

En el servidor principal se tiene activado un firewall de sistema operativo Debian 7, el cual bloquea el acceso a la red interna de aquellas páginas que no cumplen las condiciones de seguridad establecidas.

Adicionalmente se tienen antivirus con la respectiva licencia y actualizados. A pesar de esto los usuarios no tienen la precaución de analizar los dispositivos externos como memorias flash, que ingresan a las computadoras. Lo que pone en un alto riesgo de contagio a ese computador y a la red.

Los sitios web riesgosos, están bloqueados desde el servidor.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

6.5 Respaldo o Back-Up

6.5.1 Recuperación de la información

[31] Referirse al Glosario de Conceptos Técnicos

No existen políticas establecidas para los respaldos.

Se han presentado problemas por la falta de políticas de respaldo y en ocasiones se ha perdido información, teniendo que invertir más recursos para generar nuevamente la información.

Existe una máquina de escritorio identificada como servidor de respaldos, en la que se copia toda la información de un equipo al ser entregado al Departamento de Sistemas, o cuando un usuario solicita que se guarde su información. Esta máquina está ubicada en el cuarto de equipos.

Cuando un usuario necesita acceder a la información respaldada de su computador solicita autorización al responsable del Departamento de Sistemas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

6.6 Gestión de seguridad de la red

Al estar la información de la Compañía en varios servidores externos, disminuyen cualquier situación de riesgo; adicionalmente existe el firewall del sistema operativo Debian 7, habilitado en el servidor de virtualización.

Todo lo relacionado con Sistemas: hardware, software, comunicaciones, red; están a cargo de una solo persona. No existe ningún documento escrito acerca de la red; sólo esa persona sabe su configuración y funcionamiento.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

6.6.2 Seguridad de los servicios de la red

Al contar con un contrato de hosting compartido, la seguridad de la información está comprometida. Dentro de los términos del contrato, el proveedor del servicio tiene la facultad de acceder a la información con el objetivo de archivos infectados, códigos maliciosos, etc. Lo que pone en riesgo la integridad y confidencialidad de la información.

De acuerdo a la configuración de la red, el servidor de virtualización, además de cumplir con sus funciones propias, cumple las funciones de proxy y de firewall. Esto constituye una gran vulnerabilidad. Si se presenta alguna falla que lo inutilice, toda la red dejaría de operar, incluidos los servicios de red.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

6.7 Gestión de medios

6.7.1 Gestión de medios removibles

No existe un procedimiento establecido para la gestión de medios removibles, en lo referente a la seguridad, al resguardo, a procedimientos de encriptación y al buen uso que le podría dar a la información respaldada.

Algunos departamentos cuentan con unidades de almacenamiento portátiles y respaldan su información de acuerdo a sus requerimientos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

6.7.2 Eliminación de medios

Todos los activos de hardware, a pesar de estar dados de baja, permanecen en la bodega de las instalaciones de la Compañía.

No existe un procedimiento para la eliminación física de los medios en caso de presentarse algún daño que sea irreparable. Estos equipos son almacenados en bodega.

Tampoco existen procedimientos definidos para eliminar completamente la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

6.7.3 Procedimientos para el manejo de información

La información sensible está almacenada en servidores remotos. A estos servidores se puede acceder si se cuenta con una autorización previa.

Los especialistas contratados para ciertos proyectos tienen información correspondiente, únicamente a ese estudio.

El servidor de respaldos tiene una clave de acceso manejada por el responsable del Departamento de Sistemas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 70%.

6.7.4 Seguridad de la documentación del sistema

No existe documentación del sistema. Existiendo una dependencia de la persona encargada del funcionamiento de la red.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

6.8 Intercambio de información

6.8.1 Políticas y procedimientos de intercambio de información

No existe una política definida, sin embargo se realiza lo siguiente:

La entrega de información a clientes, siempre va junto a un oficio de ese proyecto, firmado por el Director del Proyecto.

Generalmente para la entrega de información a los especialistas se hace por correo electrónico, y si el volumen de la información es grande, al menos un comunicado por este medio y la información digital a través de medios removibles, y no existe ningún tratamiento especial para el intercambio de información sensible, por ejemplo encriptación de la información.

Cuando se entrega un copia de la información generada por ACOTECNIC a algún especialista, se llena un documento en el cual se detalla la información entregada, con las firmas del quien entrega y a quien se entrega. Esto no se hace en todos los casos por falta de conciencia del personal.

El responsable del Departamento Sistemas puede acceder a toda la información. Por disposición de Gerencia, dicha persona se encarga de la custodia de todas las claves.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

6.8.2 Acuerdos de intercambio

Existen acuerdos, pero ninguno establece requerimientos para la seguridad de la información. Los acuerdos se relacionan a la política de calidad (entrega – recepción documentada) y cumplimiento de cronogramas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

6.8.3 Medios físicos en tránsito

No se tienen establecidos procedimientos de medios físicos en tránsito. No existe una persona designada para la recepción, custodia y transporte de la información.

La información enviada en los medios físicos no cuenta con las seguridades debidas, los archivos no son encriptados. Tampoco se establecen compromisos de confidencialidad, no divulgación e integridad, por parte de las personas que se encargan del transporte de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

6.8.4 Mensajes electrónicos

Únicamente el personal de planta tiene una cuenta de correo de ACOTECNIC, sin embargo no existe el compromiso adecuado de salvaguardar la información. Esto constituye una vulnerabilidad latente.

Actualmente solo existe una pequeña capacitación verbal acerca del uso del correo electrónico a nuevos usuarios por parte del responsable del Departamento de Sistemas. No existen políticas del buen uso del correo electrónico.

No se utiliza sistemas de cifrados para el envío de información, a través de mensajes electrónicos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

6.8.5 Sistemas de información comercial

La información de estrategias y ofertas comerciales es resguardada por el Departamento de Preparación de Ofertas. La vulnerabilidad de la red pone en riesgo la integridad de esta información.

El servicio de internet es compartido debido a que se cuenta con un único proveedor. Si el ancho de banda se satura, se pondría en riesgo las transacciones comerciales electrónicas realizadas a través del portal de compras públicas, especialmente los procesos de subasta inversa los cuales se realizan en fechas y horas previamente establecidas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

6. 9 Servicios de comercio electrónico

6.9.1 Comercio electrónico y 6.9.2 Transacciones en-línea

La adquisición de algunas licencias y equipos se realiza a través de transacciones online. La seguridad en estas operaciones se basa en el uso de protocolos y

certificados de seguridad con los que cuentan la mayoría de sitios dedicados a las transacciones electrónicas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

6.9.3 Información públicamente disponible

La información de la Compañía publicada a través de su página web www.acotecnic.com, ha sido preparada por el personal asignado para ello, y aprobada por la Gerencia y Presidencia.

Sin embargo en esta página web se muestran también fotografías que evidencian el potencial tecnológico con el que cuenta la Compañía, para el desarrollo de sus actividades. Esta información podría ser mal utilizada, ya que desde la web se puede tener una idea de la cantidad y ubicación de computadores, laptops, impresoras, plotters, el acceso a algunas áreas de la Compañía y una idea de las seguridades físicas de las oficinas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

6.10 Monitoreo

6.10.1 Registro de auditoría y 6.10.2 Uso del sistema de monitoreo

El monitoreo lo realiza el responsable del Departamento de Sistemas semanalmente, sin embargo no se cuenta con una política y tampoco se ha definido la forma en que pueden ser utilizados estos reportes de monitoreo para fines disciplinarios.

Ante un incidente los reportes de monitoreo son solicitados por la Gerencia como base para generar un llamado de atención.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 70%.

6.10.3 Protección del registro de información

Los reportes resultantes del monitoreo son almacenados y custodiados por el responsable del Departamento de Sistemas. Los archivos son enviados a través de correo electrónico a la Administración.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 70%.

6.10 4 Registros del administrador y operador

No existen políticas definidas para cumplir este control. El responsable del Departamento de Sistemas tiene privilegios de administrador del sistema.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 5%.

6.10.5 Registro de fallas

No se tiene ningún procedimiento establecido para el registro de fallas. Sin embargo se tiene almacenados los registros resultantes del monitoreo.

Ante una falla del sistema, se genera un reporte para dar a conocer a la Administración lo sucedido.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

6.10.6 Sincronización de relojes

Las computadoras de ACOTECNIC no se encuentran con una sincronización de reloj.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 5%.

7. CONTROL DE ACCESOS

7.1 Requisitos de negocio para el control de accesos

7.1.1 Política de control de accesos

El Departamento de Sistemas intenta restringir el acceso a ciertos sitios web, pero al no existir un compromiso de parte de los empleados para el correcto uso de los activos y el apoyo de un procedimiento disciplinario, se dificulta aplicar este control.

El Departamento de Sistemas tiene restringido desde los computadores el acceso a otras máquinas, a las impresoras y al plotter. En el caso del acceso a las impresoras, simplemente no está instalado el controlador de ese equipo.

Para el acceso a la plataforma de gestión de tareas se lo realiza mediante la autentificación de usuario. Para la asignación de un usuario en la plataforma de tareas se hace una solicitud formal al Director del Proyecto. El control del acceso a esta plataforma se dificulta, si es que el usuario no maneja con responsabilidad su usuario y contraseña.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

7.2 Gestión de acceso de usuarios

7.2.1 Registro de usuarios y 7.2.2 Gestión de privilegios

Para iniciar una sesión de trabajo desde los computadores de la Compañía, es necesaria una validación de usuario y contraseña.

Existen usuarios con privilegios para acceder a la información sensible almacenada en los servidores remotos y a la plataforma de trabajo.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 70%.

7.2.3 Gestión de contraseñas de usuario

Cumpliendo una disposición de la Administración, se crearon contraseñas para el acceso a los equipos ya que se dieron casos en los que el personal de apoyo ocupaba los equipos de los empleados para asuntos personales.
Las contraseñas personales de las computadoras son del conocimiento del responsable del Departamento de Sistemas y el Departamento de Talento Humano. Se solicitó entregar las contraseñas a estas personas luego de algunos inconvenientes que se produjeron, cuando uno de los empleados abandonó su puesto de trabajo; se necesitaba información urgente del equipo y no fue posible obtenerla a tiempo por falta de la clave de acceso.

Cuando se asigna una cuenta de correo, se otorga una contraseña temporal que luego es modificada por cada usuario.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 70%.

7.2.4 Revisión de los derechos de acceso de los usuarios

ACOTECNIC no tiene un proceso formal para la revisión periódica de los derechos de acceso y privilegios de los usuarios.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

7.3 Responsabilidades de los usuarios

7.3.1 Uso de contraseñas

ACOTECNIC no tiene normas sobre la confidencialidad de sus claves de acceso. No se existen recomendaciones respecto al uso y la selección de contraseñas seguras.

No se ha realizado campañas de concientización sobre la seguridad de la información.
Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

7.3.2 Equipo informático de usuario desatendido

No se cuentan con políticas de inactivación de la estación por equipo desatendido. En la mayoría de casos ni siquiera se cuenta con una contraseña para protector de pantalla

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

7.3.3 Política de pantalla y escritorio limpio

No se cuenta con buenas prácticas de seguridad para escritorios limpios; ni para seguridad de impresiones o fotocopiados desatendidos.

Esto constituye una vulnerabilidad ya que puede existir fuga de información.

La documentación impresa para la ejecución de una actividad de revisión, se acumula como papel para reciclaje y luego es desechada como basura. Algunos departamentos realizan un adecuado proceso de destrucción de la información impresa.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

7.4 Control de acceso a la red

7.4.1 Política de uso de los servicios de la red

No se cuentan con políticas formales, pero la potestad de autorizar el acceso a la red o al servicio de red es del responsable del Departamento de Sistemas, en base a los requerimientos de cada proyecto.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

7.4.2 Autentificación de usuario para conexiones externas

Este control no es aplicable en la Compañía. El responsable del Departamento de Sistemas es la única que accede remotamente a los diferentes equipos pero únicamente en el caso de estar en las oficinas de proyectos en otras ciudades.

El acceso remoto no se aplica como una herramienta de trabajo por desconocimiento de las ventajas ofrecidas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

7.4.3 Identificación de equipos en las redes

La única restricción que se tiene para equipos que quieran conectarse al servicio de internet mediante conexión inalámbrica es la contraseña, pero en la mayoría de casos basta con preguntar a algún empleado esta información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

7.4.4 Diagnostico remoto y configuración de protección de puertos

Este control no se aplica a la Compañía ya que no se realizan estas actividades.
No se considera este control para el análisis de la situación actual de la Compañía.

7.4.5 Segregación en las redes

Todas las computadoras comparten la misma red y no se cuenta son políticas para segregar a los usuarios, sin embargo existen usuarios con diferentes privilegios de acceso, dependiendo de la función que realizan.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

7.4.6 Control de conexión a las redes

Control

Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deberían basar en los requisitos de las aplicaciones del negocio.

Análisis: No existe control de conexiones a las redes.

Para el análisis de la situación actual de la Compañía no se considera que este control.

7.4.7 Control de enrutamiento en la red

No se cuenta con controles de enrutamiento en la red.

Los equipos están conectados a la red interna está conectada a través de switch capa 2.
Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 1%.

7.5 Control de acceso al sistema operativo

7.5.1 Procedimientos de conexión de terminales y 7.5.2 Identificación y autenticación del usuario

No existe una política definida para procedimientos de conexión de terminales.

Para iniciar la sesión de cada estación de trabajo, el acceso al correo electrónico de la Compañía, el acceso a la plataforma de gestión de tareas (residentes en servidores remotos); se necesita de la autentificación de los usuarios mediante contraseñas.

Generalmente el sistema permite hasta tres intentos fallidos para el acceso, caso contrario se bloquean durante un tiempo determinado (treinta minutos). No existe un procedimiento en caso que se requiera acceder durante los periodos de bloqueo.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

7.5.3 Sistema de gestión de contraseñas

No existe un sistema para la gestión de contraseñas. No se controla que las contraseñas sean cambiadas cada cierto tiempo, ni el nivel de seguridad de las contraseñas.

Las contraseñas personales de las computadoras son del conocimiento del responsable del Departamento de Sistemas y el Departamento de Talento Humano.

Cuando se asigna una cuenta de correo, se otorga una contraseña temporal que luego es modificada por cada usuario.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

7.5.4 Utilización de las facilidades del sistema

Se crean perfiles de usuarios de tal manera que se pueda controlar la administración de estaciones de trabajo, sin embargo algunos usuarios si son administradores de sus computadoras, lo que dificulta su control.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

7.5.5 Desconexión automática de sesiones

La desconexión automática de sesiones luego de un período definido de inactividad se aplica para las conexiones a los servidores remotos. Sin embargo en la intranet no se realiza ninguna desconexión, por lo que la sesión permanece abierta durante el tiempo que el equipo esté en operación.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

7.5.6 Limitación del tiempo de conexión

Dentro de la plataforma de tareas se tiene un tiempo de 10 minutos, si no se registra movimiento dentro de este tiempo la sesión se cerrará.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

7.6 Control de acceso a las aplicaciones y la información

7.6.1 Restricción de acceso a la información

No existe una política de control de accesos definida.

Únicamente el acceso a los servidores remotos y a la plataforma de trabajos cuenta con restricciones de uso.

Para facilitar las labores de proveedores externos, la Compañía les permite el acceso a la red, por medio del Access Point, sin ninguna restricción.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

7.6.2 Aislamiento de sistemas sensibles

La información sensible se encuentra en un entorno aislado, en servidores remotos. En la intranet, los equipos no están en entornos separados, presentándose una amenaza para el acceso a la información sensible, que pudiera estar almacenada temporalmente en las estaciones de trabajo, para actividades de revisión o actividades realizadas en ese momento.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

7.7 Informática móvil y teletrabajo

7.7.1 Informática móvil y comunicaciones, y 7.7.2 Teletrabajo

No se cuenta con políticas que regulen el uso de dispositivos móviles como portátiles, agendas, teléfonos móviles y tablets, para el procesamiento y almacenamiento de la información. Tampoco existen acuerdos de confidencialidad, buen uso, no divulgación y eliminación de la información a utilizarse en este tipo de dispositivos

No se cuenta con procedimientos de seguridad o requisitos de protección física, controles de acceso, técnicas de encriptación, respaldo y protección antivirus. La protección, en muchos casos, se limita a las claves de acceso que pudieran tener estos dispositivos.

No existen reglas o procedimientos a considerarse cuando se utilizan estos dispositivos en lugares públicos o cuando se conectan a redes de acceso público, como por ejemplo WiFi en centros comerciales, parques, aeropuertos.

El respaldo de información de estos dispositivos debe hacerse con mayor frecuencia, ya que tiene más probabilidades de dañarse, extraviarse o ser víctimas de la delincuencia.

Para establecer una comunicación entre o con estos dispositivos móviles, no se ejecutan procedimientos de conectividad seguros, por ejemplo: establecimiento de túneles virtuales, autentificación de equipos mediante una dirección MAC, autentificación de usuario, etc.

En algunos proyectos se realizan reuniones de teletrabajo con técnicos de otras ciudades. Generalmente son video llamadas vía skype.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

8. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

8.1 Requisitos de seguridad de los sistemas

8.1.1 Análisis y especificación de los requisitos de seguridad

Todos los requerimientos de hardware y software de la Compañía son canalizados a través del Departamento de Sistemas. Es una buena práctica ya que se cuenta con la asesoría de un técnico, pudiendo garantizarse los requisitos de seguridad, estabilidad y disponibilidad de los activos a adquirirse.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

8.2 Seguridad de las aplicaciones del sistema

8.2.1 Validación de los datos de entrada y 8.2.2 Control del proceso interno

Cuando se establece que la Compañía debe recibir información cómo base para el desarrollo de sus actividades, la información es revisada para comprobar la integridad, compatibilidad con las herramientas de procesamiento y si es la información requerida.

Una vez que la información es validada se procede con el tratamiento de la misma y con la entrega a los especialistas externos, para que empiecen sus actividades.

Para respaldar la entrega o recepción de información, se elabora un documento el cual es firmado por las partes intervinientes. Estos procedimientos se realizan para cumplir la política de calidad, sin considerar aspectos relacionados con la seguridad de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

8.2.3 Integridad de mensajes

Control

Se debería identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones y se deberían de identificar e implementar controles apropiados.

Análisis: No existen controles para la integridad de mensajes.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

8.2.4 Validación de los datos de salida

Como resultado del cumplimiento de la política de calidad, previo a la entrega de la información a los proveedores y al cliente final, los datos de salida son validados para garantizar que el proceso de la información haya sido ejecutado correctamente.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

8.3 Controles criptográficos

8.3.1 Política de uso de los controles criptográficos

Control

La organización debería desarrollar e implementar una política de uso de las medidas criptográficas para proteger la información.

Análisis: No existen controles criptográficos dentro de ACOTECNIC. Lo que pone en riesgo la integridad de la información y la expone a mal uso o un apropiamiento indebido.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

8.3.2 Gestión de claves

Control

La gestión de claves criptográficas debe apoyar el uso de las técnicas criptográficas en la organización.

Análisis: No se maneja un procedimiento para gestión de claves de encriptado. No se dispone de controles para el encriptado de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

8.4 Seguridad de los archivos del sistema

8.4.1 Control del software en producción

Todos los usuarios tienen privilegios de Administradores de las computadoras que les han sido asignadas. La Compañía proporciona los equipos con el software propietario necesario para las actividades de trabajo. Sin embargo algunos empleados instalan programas adicionales, versiones trial o versiones no originales que ponen en riesgo la estabilidad del Sistema Operativo y comprometen la Políticas de Calidad de la Compañía.

Respecto a la seguridad, el uso de este tipo de software requiere de actualizaciones, activaciones online o la instalación de paquetes adicionales, constituyéndose esto, en un riesgo debido a que es necesario descargarlos de internet, desde sitios no seguros y que pueden contener códigos maliciosos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

8.4.2 Protección de los datos de prueba del sistema

Control

Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados.

Análisis: Los sistemas de prueba usualmente requieren de volúmenes substanciales de datos de prueba que sean lo más parecidos a los datos operacionales. El encargado de realizar las pruebas del sistema operativo, los activos de información y todos los equipos de red es el responsable del Departamento de Sistemas. Para efectos de cumplir la normativa de gestión de calidad, estos eventos son documentados y puestos en conocimiento de los Administradores de la Compañía.

Los datos de prueba y los procedimientos de prueba, no son conocidos por los usuarios.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 70%.

8.4.3 Control de acceso al código fuente de los programas

ACOTECNIC no desarrolla software. Utiliza aplicaciones especializadas existentes, haciendo uso de las diferentes librerías disponibles o implementando algunas, para cumplir con los requerimientos de un estudio.

Para el análisis de la situación actual de la Compañía no se considera que este control.

8.5 Seguridad en los procesos de desarrollo y soporte

8.5.1 Procedimientos de control de cambios, 8.5.2 Revisión técnica de los cambios en el sistema operativo y 8.5.3 Restricciones en los cambios a los paquetes de software

ACOTECNIC no desarrolla software. Utiliza aplicaciones especializadas existentes, haciendo uso de las diferentes librerías disponibles o implementando algunas, para cumplir con los requerimientos de un estudio.

Para el análisis de la situación actual de la Compañía no se considera que este control.

8.5.4 Fuga de Información

ACOTECNIC no cuenta con controles para la protección de la información. Ante la carencia de estos controles resulta fácil extraer la información sin que existan ningún tipo de alertas.

No existe restricción alguna para el almacenamiento de datos en dispositivos removibles como memorias USB, discos duros externos, iPods, etc.; ni para la escritura en unidades CD/DVD. Tampoco se maneja la encriptación de datos almacenados en dispositivos removibles.

Actualmente los colaboradores no tienen deshabilitado los puertos USB y es por esta vía que se podría extraer información valiosa. No se controla la información que es transmitida por correos electrónicos o que es respaldada en la nube.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

8.5.5 Desarrollo externo del software

ACOTECNIC no desarrolla software. Utiliza aplicaciones especializadas existentes, haciendo uso de las diferentes librerías disponibles o implementando algunas, para cumplir con los requerimientos de un estudio.

Sin embargo los proveedores externos elaboran librerías para automatizar su trabajo. Dentro de los contratos de prestación de servicios, la información que ACOTECNIC recibe no incluye la entrega de estas librerías o de alguna otra aplicación de software; por lo que este control no es aplicable a la Compañía.

Para el análisis de la situación actual de la Compañía no se considera que este control.

8.6 Gestión de la vulnerabilidad técnica

8.6.1 Control de las vulnerabilidades técnicas.

Se realiza un monitoreo de las vulnerabilidades técnicas por parte del responsable del Departamento de Sistemas, no obstante la Administración no ha tomado las medidas correctivas adecuadas.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 40%.

9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

9.1 Reportando eventos y debilidades de la seguridad de información

9.1.1 Reportando los eventos en la seguridad de información

Control

Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada

No está establecido ningún procedimiento para reportar estos eventos. Sin embargo el responsable del Departamento de Sistemas elabora los reportes respectivos y los pone en conocimiento de la Administración.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

9.1.2 Reportando debilidades en la seguridad de información

Control

Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.

Análisis: A excepción del responsable del Departamento de Sistemas, no se reportan debilidades en la seguridad de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

9.2 Gestión de las mejoras e incidentes en la seguridad de información

9.2.1 Responsabilidades y procedimientos

ACOTECNIC no cuenta con procedimientos formales para que el personal actúe ante un evento de incidente de seguridad de la información. No se tienen definidas las responsabilidades ante un evento de seguridad

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

9.2.2 Aprendiendo de los incidentes en la seguridad de información

No existe ningún documento acerca del detalle de incidente, en qué afectó, cuál fue el impacto que causó, un informe de cómo lo resolvieron.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 5%.

9.2.3 Recolección de evidencia

El Departamento de Sistemas no cuenta con un proceso para el tratamiento y custodia de las evidencias ante un incidente de seguridad. No se tiene registros de las evidencias.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 60%.

10. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

10.1 Aspectos de la gestión de continuidad del negocio

10.1.1 Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio

Control

Se debería instalar en toda la organización un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del negocio a través de la organización que trate los requerimientos en la seguridad de información necesarios para la continuidad del negocio.

Análisis: No se ha establecido ninguna política o proceso que ayude a mantener la continuidad del negocio en caso de presentarse algún evento.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

10.1.2 Continuidad del negocio y evaluación de riesgos

Al fugarse la información, la asignación de los proyectos podría verse afectada ya que se pierde la ventaja competitiva acumulada por la Compañía en la ejecución de los proyectos durante su vida institucional.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

10.1.3 Redacción e implantación de planes de continuidad que incluyen la seguridad de información

Control

Se deberían desarrollar planes de mantenimiento y recuperación de las operaciones del negocio, para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos.

Análisis: No existen planes de este tipo.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

10.1.4 Marco de planificación para la continuidad del negocio

Control

Se debería mantener un esquema único de planes de continuidad del negocio para asegurar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.

Análisis: No existe alguna planificación de este tipo.
Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

10.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

Control

Los planes de continuidad del negocio se deberían probar regularmente para asegurarse de su actualización y eficacia.

Análisis: No están definidos planes de continuidad.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 10%.

11. CUMPLIMIENTO

RESULTADOS DE LA EVALUACIÓN: Al no contar con una política definida, el cumplimiento no existe, sin embargo para referencia se enlistan los controles que comprenden este dominio.

11.1 Cumplimiento con los requisitos legales

11.1.1 Identificación de la legislación aplicable

La Compañía cuenta con la asesoría de profesionales del Derecho, quienes asesoran a los Administradores en materia legal sobre las áreas laboral, civil entre otros.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 70%.

11.1.2 Derechos de propiedad intelectual (DPI)

Los proyectos desarrollados tienen la firma de autoría y responsabilidad de ACOTECNIC. La información permanece en la oficina de la Compañía, mas el dueño de la información es el cliente que contratante.

Las copias realizadas de los estudios, se efectuarán previa solicitud del cliente.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 20%.

11.1.3 Salvaguarda de los registros de la organización

La salvaguarda de los registros se relaciona con el manejo que hace la política de calidad al respecto. Existe una clasificación de registros contables, transacciones, auditoría, procedimientos operativos; mas no orientados a la seguridad de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 50%.

11.1.4 Protección de los datos y de la privacidad de la información personal

No está establecida una política organizacional de privacidad y de protección de datos personales.

En las computadoras asignadas a los empleados existe información personal que en ocasiones es respaldada conjuntamente con la información perteneciente a la Compañía, produciéndose, además un consumo inadecuado de los recursos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

11.1.5 Prevención en el mal uso de los recursos de tratamiento de la información

No existe el concepto claro sobre la propiedad de los recursos y de la información de la Compañía por parte del personal; utilizando en ocasiones estos elementos para fines personales.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 30%.

11.1.6 Regulación de los controles criptográficos

Control

Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.

Análisis: La Compañía no cuenta con controles criptográficos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

11.2 Revisiones de la política de seguridad y de la conformidad técnica

11.2.1 Conformidad con la política de seguridad y los estándares

Control

Los gerentes deberían asegurarse que se cumplan correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad cumpliendo las políticas y estándares de seguridad.

Análisis: No existen procedimientos de seguridad de la información definidos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

11.2.2 Comprobación de la conformidad técnica

Control

Se debería comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información.

Análisis: No existen procedimientos de seguridad de la información definidos.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

11.3 Consideraciones sobre la auditoria de sistemas

11.3.1 Controles de auditoría de sistemas

Control

Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.

Análisis: No se realizan auditorías de sistemas relacionados con la seguridad de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

11.3.2 Protección de las herramientas de auditoría de sistemas

Control

Se deberían proteger los accesos a las herramientas de auditoría de sistemas con el fin de prever cualquier posible mal uso o daño.

Análisis: No se cuenta con herramientas de auditorías de sistemas relacionados con la seguridad de la información.

Para el análisis de la situación actual de la Compañía se considera que este control se cumple en un 0%.

12 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA COMPAÑÍA

En Administración de Empresas, se utiliza el cálculo de indicadores, similares a los que podría utilizarse en la medición de gestión, para el análisis y estudio de un control de seguridad determinado y las posibles mejoras de cambio que se generen luego de la implementación de políticas, procedimientos, mejoras de red, incluyendo características cuantitativas y cualitativas.

Se ha estimado, en forma conjunta con funcionarios de la Compañía, un porcentaje de cumplimiento de cada uno de los controles para la seguridad de la información que recomienda las Norma ISO/IEC 27002.

De acuerdo a la estructura de la Norma ISO/IEC los 133 controles se agrupan en 39 objetivos de control y estos a su vez se organizan en 11 dominios.

Es necesario considerar que no todos los objetivos de control ni todos los dominios tienen la misma importancia en las actividades de la Compañía, por lo que se ha establecido un factor denominado “PESO”, que nos permitirá incluir la importancia que se estima para cada dominio y objetivo dentro de la Compañía.

En la tabla 4.1 se registra el PESO estimado para cada uno de los 11 Dominios utilizados en el presente estudio. Se considera una escala de 1 (menor importancia) a 5 (mayor importancia).

DOMINIOS DE LA SEGURIDAD DE LA INFORMACIÓN	PESO (IMPORTANCIA)
1. POLÍTICA DE SEGURIDAD.	5
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	4

3. GESTIÓN DE ACTIVOS.	5
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	4
5. SEGURIDAD FÍSICA Y DEL ENTORNO.	3
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	5
7. CONTROL DE ACCESO.	4
8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	2
9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	2
10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	3
11. CUMPLIMIENTO.	3

Tabla 4.1 Peso estimado para cada Dominio

Se puede observar que los aspectos más importantes para la situación de la Compañía son el establecimiento de las políticas de seguridad, la gestión de activos y la gestión de comunicaciones y operaciones.

En el caso de los 39 objetivos de control se ha estimado un PESO entre 1 y 10, de tal forma que los objetivos que pertenecen a un mismo dominio, no sobrepasen el índice máximo de cumplimiento (10).

Ejemplo:

- El dominio “1. POLÍTICA DE SEGURIDAD” tiene un solo objetivo de control por lo que el PESO se ha elegido 10.

- El dominio “2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN” tiene dos objetivos de control, al primer objetivo se le ha asignado un peso de 6, y al segundo un peso de 4. Entre los dos suman 10.

DOMINIOS y Objetivos de control	PESO DOMINIO	PESO OBJETIVO DE CONTROL
1. POLÍTICA DE SEGURIDAD.	10	
1.1 Política de seguridad de la información.		10
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	10	
2.1 Organización interna.		6
2.2 Terceros.		4
3. GESTIÓN DE ACTIVOS.	10	
3.1 Responsabilidad sobre los activos.		5
3.2 Clasificación de la información.		5
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	10	
4.1 Antes del empleo.		2
4.2 Durante el empleo.		3
4.3 Cese del empleo o cambio de puesto de trabajo.		5
5. SEGURIDAD FÍSICA Y DEL ENTORNO.	10	
5.1 Áreas seguras.		4
5.2 Seguridad de los equipos.		6
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	10	
6.1 Responsabilidades y procedimientos de operación.		1
6.2 Gestión de la provisión de servicios por terceros.		1
6.3 Planificación y aceptación del sistema.		1
6.4 Protección contra el código malicioso y descargable.		1
6.5 Copias de seguridad.		1
6.6 Gestión de la seguridad de las redes.		1
6.7 Manipulación de los soportes.		1
6.8 Intercambio de información.		1
6.9 Servicios de comercio electrónico.		1
6.10 Supervisión.		1
7. CONTROL DE ACCESO.	10	
7.1 Requisitos de negocio para el control de acceso.		2
7.2 Gestión de acceso de usuario.		2
7.3 Responsabilidades de usuario.		1
7.4 Control de acceso a la red.		2
7.5 Control de acceso al sistema operativo.		1
7.6 Control de acceso a las aplicaciones y a la información.		1
7.7 Ordenadores portátiles y teletrabajo.		1
8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	10	
8.1 Requisitos de seguridad de los sistemas de información.		2
8.2 Tratamiento correcto de las aplicaciones.		2
8.3 Controles criptográficos.		2
8.4 Seguridad de los archivos de sistema.		1
8.5 Seguridad en los procesos de desarrollo y soporte.		1
8.6 Gestión de la vulnerabilidad técnica.		2
9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	10	
9.1 Notificación de eventos y puntos débiles de seguridad de la información.		5
9.2 Gestión de incidentes y mejoras de seguridad de la información.		5
10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	10	
10.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.		10
11. CUMPLIMIENTO.	10	

11.1 Cumplimiento de los requisitos legales.		4
11.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.		4
11.3 Consideraciones sobre las auditorías de los sistemas de información.		2

Tabla 4.2: Pesos asignados a los Objetivos de Control

Con los porcentajes de cumplimiento y los pesos estimados se ha podido determinar que el porcentaje de cumplimiento de la Compañía, en la actualidad, es del **30.42%.**

Los dominios que presentan un mayor índice de cumplimiento, son los relacionados a la gestión de activos y la gestión de comunicaciones. Esto, debido al cumplimiento de la Política de Calidad, que exige se mantenga un control documentado de activos y procedimientos de entrega de información.

Los dominios que presentan un menor índice de cumplimiento, son los relacionados al cuidado y manejo de la información, gestión de la continuidad del negocio, y la implementación de la política de seguridad de la información.

Representando gráficamente el cálculo de los índices de cumplimiento, se puede observar que el porcentaje de cumplimiento en términos generales es bajo. Con esta representación podemos observar que es preciso centrar los esfuerzos en realizar mejoras en los Dominios considerados importantes de acuerdo a las necesidades de la Compañía.

En el gráfico 4.1 las barras de color azul representan la importancia del dominio y las barras de color marrón, el índice de cumplimiento actual.

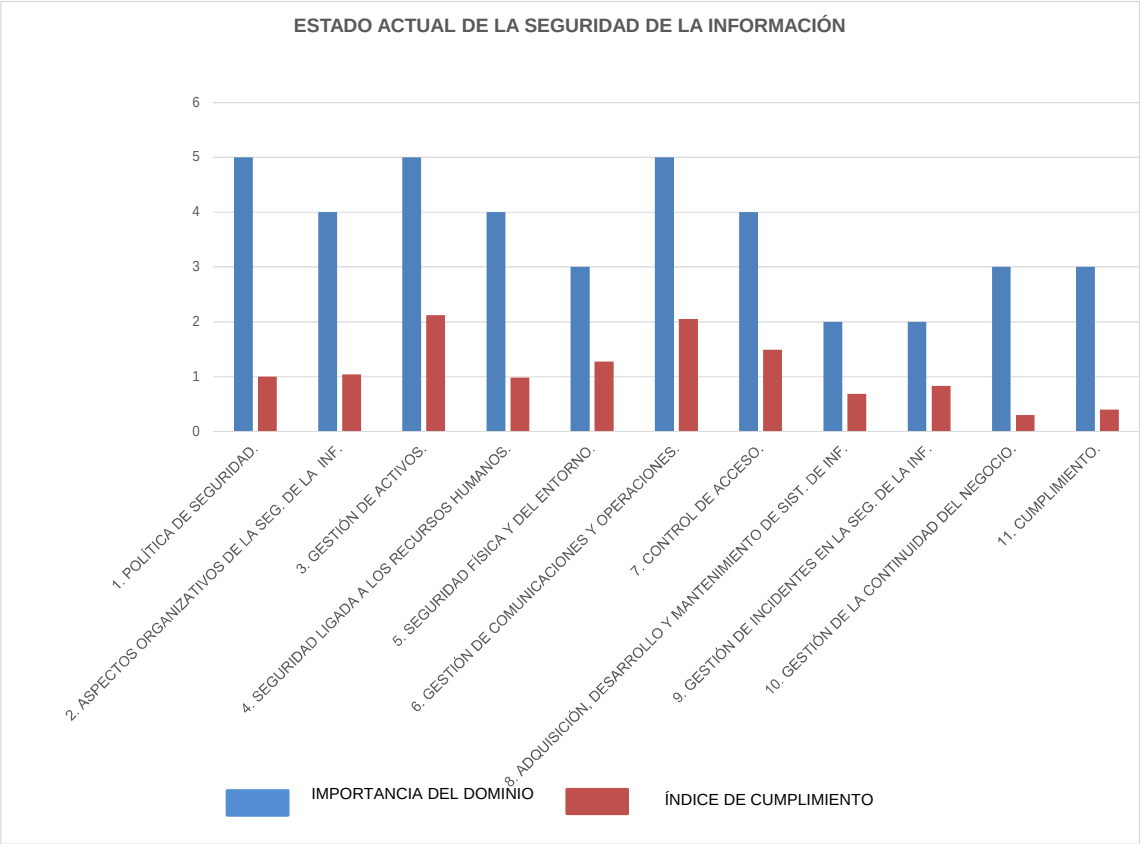


Figura: 4.1 Índices de Cumplimiento

CAPÍTULO V

Diseño de Estrategias para el Sistema de Seguridad de la Información

1. Estrategias para el Sistema de Seguridad de la Información para la Compañía ACOTECNIC Cía. Ltda.

En base al análisis realizado en el capítulo IV, se ha podido determinar que el riesgo, relacionado con la pérdida de información, al que está expuesta la Compañía, es elevado.

Es preciso definir una política de seguridad de información clara, que sea conocida por todos los involucrados en las actividades de ACOTECNIC. Se propone, de acuerdo a los requerimientos de la Compañía, el siguiente plan de seguridad para prevenir y reducir al máximo el impacto de estos eventos en la continuidad del negocio.

1.1 Implementación de Políticas de Seguridad de la Información.

La Administración debe establecer políticas puntuales, factibles, de carácter obligatorio; que faciliten la implementación de un Sistema de Gestión de Seguridad de la Información, de acuerdo a sus necesidades.

Cada política debe ser difundida a todos los involucrados en el negocio: personal de planta, personal de apoyo, personal contratado temporalmente, proveedores especialistas externos, clientes y toda persona que tenga acceso a los activos de la Compañía.

Se recomienda considerar los siguientes aspectos, en dicha política:

- Una introducción a la seguridad de la información, que exponga los aspectos más relevantes y exprese la importancia de la Gestión de Seguridad de la Información.
- Objetivo (s), alcance, definición de conceptos básicos.
- Debe tener conformidad con los requisitos establecidos por las leyes, normas y reglamentos vigentes en el País.
- La forma de evaluar los riesgos y la gestión de los mismos
- Consecuencias de las violaciones de seguridad de la información.
- Procedimientos para informar sobre un incidente ocurrido, a la persona responsable de la seguridad de la información.

Teniendo en cuenta los diferentes escenarios que maneja la Compañía en sus actividades operativas, comerciales, relación con proveedores y clientes, se sugiere se establezcan como base del Sistema de Seguridad de la Información, las siguientes políticas:

- Política de clasificación de la información.
- Política de protección y acceso a la información.
- Política para el manejo de la información por parte de terceros y clientes.
- Política de destrucción de la información.
- Política de almacenamiento y recuperación de la información.
- Política para la Gestión de Recursos Humanos
- Política de control de accesos y uso de las TICs
- Política de uso apropiado de los servicios de red

Estas políticas pueden complementarse con:

- Política de protección de datos y privacidad de información personal.
- Política para la gestión de la continuidad del negocio

- Política para el tratamiento de incidentes de seguridad
- Política de seguridad física.

1.2 Política de clasificación de la información

Debe contener los criterios y procedimientos necesarios para cuantificar y clasificar toda la información de la Compañía, de acuerdo a su sensibilidad y el valor dentro de los procesos operativos y administrativos de la Compañía.
Una clasificación podría ser:

- **Información pública de carácter general:** que no requiere restricciones en el acceso y puede darse a conocer al público en general, por ejemplo: información de la página web, presentación de la Compañía, oferta de servicios, capacidad técnica operativa, experiencia y trabajos ejecutados, datos de contacto.
- **Información pública corporativa:** información que puede ser comunicada sin restricciones a los involucrados en las actividades de la Compañía, por ejemplo: comunicados, instrucciones y directrices de carácter administrativo y operativo, reglamentos y procedimientos internos, capacidad técnica operativa, distributivo de personal, directorios telefónicos, roles y responsabilidades de cada empleado.
- **Información sensible:** Información que debe ser protegida debido a su importancia en los procesos operativos, administrativos y comerciales de la Compañía, por ejemplo: Bases de datos contables, preparación de ofertas, resultados de estudios, estrategias de negocios, etc. Información que por obligación contractual debe tener este tratamiento.

Las personas que acceden a la información, tienen la obligación acotar las políticas de la Compañía.

Es preciso mantener la confidencialidad de información pública corporativa y la información sensible, al interior de la Compañía.

En la información sensible, debe considerarse además del buen uso y la confidencialidad; acuerdos adicionales de no divulgación de la información. El acceso a este tipo de información debe ser restringido y debe ser autorizado por la Administración.

La información debe clasificarse en base al impacto que podría ocasionar el mal uso, la pérdida o la destrucción de dicha información en la continuidad del negocio.

Los responsables de la información deben tener la capacidad suficiente para realizar esta clasificación. Es conveniente que cada departamento administrativo u operacional haga una primera clasificación, con los justificativos suficientes para que sea puesta en consideración de la Administración, quién mantendrá o modificará dicha clasificación en base al análisis de los justificativos y a las estrategias y objetivos del negocio.

Se debe establecer las restricciones de acceso de acuerdo al tipo de información y se deben establecer las posibles sanciones a imponerse en caso de presentarse algún incidente. Dichas sanciones deben estar en concordancia con la clasificación de la información.

1.3 Política de protección de la información

Debe contener los criterios y procedimientos necesarios para proteger la información, en cualquier forma que esta se encuentre: impresa, en archivos digitales, almacenada en dispositivos móviles, unidades de almacenamiento, etc., de forma que se garantice la integridad, autenticidad, confidencialidad y disponibilidad de la misma cuando se la necesite.

Se deben establecer, acuerdos de confidencialidad que garanticen que los activos entregados por la Compañía serán utilizados para beneficio de ACOTECNIC y no para otros fines.

Acuerdos adicionales de buen uso de activos, de no divulgación, de respeto a la propiedad intelectual, ayudan a conseguir un mayor nivel de protección.

La Compañía cuenta con un sistema de autentificación para el acceso a la información sensible almacenada en servicios "*hosting"*, especialmente la información financiera y la información de la plataforma de tareas de los proyectos, sin embargo es conveniente que se implemente un sistema de gestión de accesos en la intranet.

Se recomienda implementar controles adicionales que garanticen que las estaciones de trabajo no estén desatendidas o que las sesiones de trabajo permanezcan abiertas cuando no se las está utilizando. Así mismo es conveniente no mantener documentos con información sensible sobre los puestos de trabajo, especialmente si dichos puestos están desatendidos.

Los documentos impresos no deberían permanecer desatendidos en las impresoras por mucho tiempo, tampoco deben ser abandonados en las mismas.

En caso que los dispositivos de impresión y escaneo, cuenten con funciones de almacenamiento de archivos en memoria interna, dichos archivos deben ser eliminados de la memoria una vez que se culmine el trabajo.

Los documentos impresos que ya no son utilizados deben ser adecuadamente destruidos o eliminados, conforme a las recomendaciones dadas en la política de destrucción de la información.

En caso de que sea necesario mantener por determinado tiempo documentos que contengan información sensible, éstos deben estar almacenados con las seguridades del caso; cajones y armarios con cerraduras, caja fuerte, permitirán mantener protegidos dichos documentos.

Unidades de almacenamiento de información y equipos de computación que vayan a ser “dados de baja” deben someterse a un proceso de formateo de bajo nivel, de forma que sea eliminada toda la información de las unidades de almacenamiento de datos.

Las comunicaciones realizadas por medio de correo electrónico deben incluir al final del cuerpo del correo las notas de descargo y confidencialidad, de tal forma que se deje constancia que el asunto tratado sólo es de interés de las personas incluidas en dicha comunicación.

Es necesario definir los procedimientos necesarios para mantener respaldo de la información, principalmente las versiones finales de proyectos ya entregados, así como la persona responsable de la custodia y almacenamiento de la misma.

Es necesario que se establezcan las instrucciones necesarias para evitar que información sensible sea almacenada en los equipos de computación y procesamiento individual, es recomendable que este tipo de información se mantenga en las unidades de procesamiento centralizadas, ya que estas unidades cuentan con un control de acceso más estricto.

Concientizar al personal que la información también puede estar en conversaciones y que es necesario tener precaución de revelar información sensible, tanto al interior de la Compañía como en lugares públicos, ya que personas con mala intención, pueden tomar ventaja de lo que están escuchando.

Debe evitarse el uso no autorizado de fotocopiadoras, escáner o cámaras digitales dentro de las instalaciones de la Compañía.

1.4 Política para el manejo de la información por parte de terceros y clientes.

Se deben establecer, acuerdos de confidencialidad, de buen uso de activos, de no divulgación y de respeto a la propiedad intelectual, que garanticen que los activos entregados por la Compañía serán utilizados para beneficio del proyecto al que pertenecen y no para otros fines. Estos acuerdos deben extenderse a todas las personas que pudieran tener acceso a los activos de información de la Compañía, incluyendo personal de apoyo, de mantenimiento de equipos, etc.

Se debería especificar los canales adecuados para mantener la comunicación, así como la recepción y entrega de información que se realice con proveedores externos y clientes.

Debe designarse a las personas que serán las responsables de entregar, recibir, transportar y mantener la custodia de la información de parte de la Compañía, de los proveedores externos y de los clientes.

En caso de requerirse el uso de la información para propósitos diferentes a los objetivos del proyecto, la parte interesada deberá obtener la autorización respectiva de la propietaria de dicha información. Documentos de soporte serán necesarios para respaldar dicha autorización.

Es recomendable que la información sensible se imprima, si y sólo si es estrictamente necesario. En caso de realizar copias de esta información, éstas deben ser destruidas y eliminadas adecuadamente, una vez que se haya culminado la actividad para la que fueron impresas.

Se debe contar con procedimientos claramente definidos para la entrega y traspaso de la responsabilidad de activos, en especial activos de información, a los proveedores externos y clientes finales. Estos procesos deben tener los respectivos documentos de respaldo.

1.5 Política de destrucción de la información.

El inventario de activos de hardware constantemente es actualizado; sin embargo es necesario que se defina el procedimiento a seguir con los equipos obsoletos o "dados de baja" y el tratamiento que se les debe dar respeto a la migración de datos y la eliminación de información de las unidades de almacenamiento de datos (memorias).

Los documentos impresos que no sean utilizados deben ser destruidos adecuadamente, el uso de una trituradora de papel puede ayudar en esta tarea.

Es recomendable establecer un cronograma para la destrucción de documentos físicos que contengan información, que puede ser semanal, mensual o trimestral.

El intervalo de tiempo debe seleccionarse tomando en cuenta lo dispuesto en la política de clasificación de la información.

Documentos con información sensible para el negocio, deben ser destruidos lo antes posible, si ya no van a ser utilizados. Si por algún motivo, no se puede destruir inmediatamente, por falta de equipos o por otra causa, el responsable del manejo de dichos documentos debe mantener la custodia de los mismos, tomando en cuenta las recomendaciones dadas por la política de protección de la información, hasta su destrucción final.

Cuando un empleado deba terminar su relación laboral con la empresa, deberá acatar las disposiciones dadas en la política para la gestión de recursos humanos.

Una vez que todos los activos sean devueltos y las responsabilidades transferidas a la Compañía, se podrá destruir y eliminar la información que el ex-empleado utilizaba para sus actividades, incluso la información personal almacenada en los equipos de procesamiento de la información.

Debe especificarse una instrucción expresa de prohibir la destrucción, alteración, apropiación y ocultamiento de información por parte de las personas, en caso de culminar la relación laboral, ya que podría destruirse de forma inconsciente o mal intencionada información sensible, pudiendo considerarse esto como un acto de sabotaje y derivar en un proceso judicial.

1.6 Política de almacenamiento y recuperación de la información.

La Compañía mantiene copias de seguridad de algunos computadores, principalmente de las personas que han finalizado las relaciones laborales; no obstante, dentro de estos archivos se tiene respaldo de información personal, música, videos entre otros, que ocupan espacio y que no son de utilidad para la Compañía.

Otro inconveniente es que se en ocasiones se cuenta con varias versiones de un mismo archivo, y no se cuenta con la versión definitiva.

Debe especificarse la periodicidad con la cual se hará el respaldo de información a través de la red, y cuales carpetas, contenidos de información, serán las que se respalden. Por ejemplo se puede respaldar automáticamente cada trimestre la información que se encuentre en una partición del disco, quedando fuera de estos respaldos información personal, que podría almacenarse en la carpeta “mis documentos”.

Es aconsejable que se utilicen métodos de encriptación para mantener la seguridad de la información respaldada, así como procurar una ubicación diferente a la oficina para evitar pérdida de información en caso de producirse un daño físico en las instalaciones.

Es conveniente que se determine la periodicidad de revisión de los respaldos para comprobar que los métodos de almacenamiento son adecuados y sobre todo, para verificar la validez de la información respaldada.

Se debe definir el periodo de almacenamiento máximo de la información y la forma en la cual esta información será eliminada o destruida.

1.7 Política para la Gestión de Recursos Humanos

1.7.1 Seguridad antes del empleo:

Es preciso asegurarse que los empleados, contratistas y terceros entiendan sus responsabilidades y que sean los candidatos más adecuados para los roles que han sido considerados. Esto permitirá reducir el riesgo de hurto, fraude o mal uso de los activos. Es fundamental poner en conocimiento de los candidatos, las políticas acerca de seguridad de la información, funciones de seguridad, responsabilidades y acuerdos de confidencialidad que se hayan implementado. Estas instrucciones también deben aplicarse al personal temporal, proveedores externos y terceros, que pretendan ser involucrados en las actividades de la Compañía.

La Compañía tendrá la potestad de verificar la información que consta en sus hojas de vida, en cualquier momento, en concordancia con las leyes y regulaciones, manteniendo la ética profesional y protección de datos personales.

En caso de ser necesarias pruebas a los candidatos, es fundamental poner en conocimiento y solicitar que se firmen los acuerdos de confidencialidad y no divulgación de la información a la que tengan acceso, incluyendo datos, inspección a las instalaciones, procedimientos internos, etc.

1.7.2 Durante el empleo:

Es preciso asegurarse que los empleados, contratistas y terceros estén al tanto de las políticas de seguridad de la información; y que se establezca un programa continuo de capacitación, motivación y recordatorios acerca de dichas políticas. Esto permitirá reducir los riesgos a la seguridad de la información debido al factor humano.

Una inadecuada gestión del recurso humano en relación a las políticas de seguridad de la información puede causar temor, malestar, desconfianza y poca participación del personal en los procedimientos de seguridad de la información.

Se debe establecer y comunicar, clara y oportunamente los procesos disciplinarios a aplicarse en caso de detectarse una amenaza o vulnerabilidad, los mismos que no debieran empezar a aplicarse sin una verificación previa y un correcto y justo tratamiento de las responsabilidades de lo ocurrido.

Si por algún motivo, los empleados tienen la necesidad de utilizar sus recursos computacionales personales, se debería contar con una autorización de parte de la Gerencia, además deben respetar los acuerdos de confidencialidad, no divulgación y responsabilidad del manejo y custodia de la información.

La Compañía es la propietaria de la información que se genere como resultado del trabajo ejecutado por parte de sus empleados y trabajadores, en ningún caso el empleado podrá destruir, eliminar, ocultar, alterar o tomar información sin la autorización respectiva, aún si la relación laboral no culmine de forma satisfactoria.

1.7.3 Finalización y cambio de empleo:

Es necesario asegurarse que los empleados, contratistas y terceros terminen su relación laboral con la Compañía de forma adecuada, lo que permitirá que se devuelvan y se traspasen los recursos entregados para el desarrollo de las actividades.

La devolución de activos, así como las novedades que se presenten, deben ser registradas en un documento que servirá como respaldo de la conformidad de las partes en la transferencia de propiedad y responsabilidad de los activos.

Se deberá notificar oportunamente a todos los involucrados en el negocio estos cambios en el personal.

En el caso que se estén utilizado recursos de propiedad del empleado, proveedores externos y terceros para el almacenamiento, procesamiento y custodia de información de la Compañía, se debe establecer el procedimiento adecuado para que dicha información se transferida de regreso a la Compañía, y cuáles serán los procedimientos para eliminar la información de los dispositivos personales.

En caso que un empleado, debido a la naturaleza de su cargo, sea el único poseedor de información acerca de la operación, configuración de activos; dicha información debe ser documentada y transferida a la Compañía. Se deberá contar con un documento que respalde la entrega, recepción y transferencia de información.

1.7.4 Retiro de los derechos de acceso:

Se deben retirar los permisos de acceso una vez que se haya terminado las relaciones laborales.

1.8 Política de control de accesos y uso de los recursos de red

La Compañía cuenta con un control de accesos a determinados recursos, especialmente Internet, mediante el bloqueo de algunas páginas, y restricciones para recursos de impresión mediante la instalación de los controladores, sin embargo es necesario complementar estos controles con las siguientes recomendaciones:

El control de accesos debe basarse en los requerimientos de seguridad y las actividades específicas que va a desarrollar cada usuario.

Se debe especificar el procedimiento para obtener una autorización para acceder a los recursos, incluyendo las reglas y responsabilidades.

Se debe realizar una revisión periódica de los controles de acceso, de forma que detecte a tiempo, si se están cumpliendo o no un adecuado control, especialmente del personal que ha cambiado de funciones o que ha dejado de trabajar en determinado equipo de trabajo.

1.8.1 Equipo informático desatendido:

Debe establecerse la protección necesaria de equipos cuando estén desatendidos, entre los controles a implementarse están: cancelar las sesiones activas antes de marcharse, bloqueo de sesión, protectores de pantalla con contraseña, inicio de sesión con contraseña, desconexión de sesiones después de un periodo determinado de inactividad.

1.8.1 Control y uso de los servicios de red:

Debe impedirse el uso no autorizado, así como evitar el mal uso de los mismos.

Es recomendable que se segreguen los usuarios de acuerdo a las actividades que ejecuten. Se debe establecer las redes y los servicios a los que tiene acceso cada usuario. El uso de redes VLAN o redes privadas dedicadas, limitar el ancho de banda, podría ayudar a esta segregación.

En caso de requerirse autorización para el acceso de personal externo a los servicios de red de la Compañía, es necesario definir métodos apropiados de autentificación, así como definir los privilegios de acceso.

Métodos de encriptación basados en certificaciones de máquina o establecimiento de túneles virtuales podrían ser útiles para autentificar nodos o usuarios de conexiones remotas, sin embargo estas conexiones no deben establecerse automáticamente, ya que podrían constituirse en un punto de acceso no autorizado en caso que el computador sea utilizado por otra persona diferente a un usuario autorizado.

1.8.2 Identificación de equipos en la red:

La identificación de equipos puede ser utilizada como un indicador para conocer si el equipo está autorizado para conectarse a una red, en caso de existir varias redes y particularmente si estas redes son de sensibilidad diferida.

1.8.3 Informática móvil y teletrabajo:

Por requerimientos de la Compañía, ha sido necesario mantener sesiones de trabajo con sus oficinas de otras provincias, la aplicación Skype es el medio de comunicación utilizado. Se recomienda hacer uso de túneles virtuales y dentro de estos enlaces utilizar dicha aplicación. Es conveniente que se tenga en cuenta la seguridad física de la estación remota, de forma que se evite que personas no autorizadas escuchen las sesiones virtuales de trabajo.

Al momento no se utilizan dispositivos móviles para actividades de trabajo, pero sí son utilizados por los empleados para comunicaciones, especialmente redes

sociales con fines laborales. Es conveniente permitir el acceso a este tipo de dispositivos a través de una red dedicada que cuente con las seguridades necesarias.

1.9 Política para la gestión y uso de contraseñas:

Cada usuario es responsable de la selección y utilización de su contraseña, sin embargo por política de la Compañía, actualmente se tiene un registro de todas las contraseñas, lo que compromete la confidencialidad de las mismas.

Los usuarios son responsables del buen uso de los recursos que se les han asignado, sin embargo existirán casos en los que la Compañía requiera acceder a dichos recursos, eximiendo, de alguna manera, la responsabilidad por el uso de los mismos al funcionario responsable del equipo. Cuando se presenten este tipo de eventos, es necesario documentar la fecha y hora de inicio y fin de la intervención, los motivos, las actividades realizadas y si existió o no modificación alguna en los recursos intervenidos, fundamentalmente la información. Esta información debe dársela a conocer al responsable del equipo con los respectivos documentos de respaldo.

Es recomendable que se evite el uso contraseñas que utilicen información relacionada con la vida personal del usuario, por ejemplo nombres, fechas de nacimiento, números de teléfonos, palabras que estén incluidas en diccionarios, que tengan caracteres repetidos o que estén conformadas solo por letras o solo por números.

No es conveniente que procesos automáticos, almacenen las contraseñas de forma permanente.

No se debe compartir las contraseñas y es aconsejable cambiarlas con frecuencia.

Evitar el uso de las mismas contraseñas para fines personales y asuntos de trabajo.

1.10 Política de uso apropiado de los servicios de red

Esta política procura el uso racional de los recursos necesarios para realizar las actividades de comercio electrónico, acceso a los servidores remotos y brindar disponibilidad del ancho de banda para las transacciones operativas de la Compañía a través de internet.

1.10.1 Actividades de comercio electrónico:

La Compañía trabaja con instituciones privadas y gubernamentales. La modalidad de contratación con las instituciones gubernamentales se realiza por medio del portal de compras públicas, siendo de suma importancia destinar los recursos necesarios que aseguren que dichas transacciones se puedan llevar a cabo sin inconvenientes y de forma oportuna, ya que la fecha y hora de dichos eventos son fijas.

Se debe concientizar a los trabajadores sobre la importancia comercial de estos eventos, ya que se podría perder importantes oportunidades de trabajo por la no disponibilidad de los recursos debido al mal uso de los servicios de red.

Al momento se limita el acceso a internet mediante el bloqueo de determinados sitios web, sin embargo este control podría complementarse con la implementación de redes VLAN en donde se podría establecer privilegios de acuerdo a la prioridad de actividades dentro de la Compañía. Otra forma de limitar el uso de ciertos servicios podría realizarse mediante protocolos que limiten el ancho de banda utilizado en cada sesión.

Es recomendable se implemente una conexión de respaldo, que sería utilizada en casos de emergencia, cuando la conexión principal falle, especialmente durante

los procesos de contratación dentro del portal de compras públicas. Se podría contratar un plan de datos con características residenciales con un proveedor diferente al que brinda el servicio principal.

1.10.2 Servicios de correo electrónico:

En cuanto al intercambio de información al interior de la Compañía es obligatorio el compromiso de los miembros para darle buen uso a los recursos, por ejemplo que se evite envío de correos innecesarios, reenvío de cadenas de correos, etc., así como evitar el re direccionamiento de correos corporativos hacia correos externos personales.

1.10.3 Acceso a los servicios de internet de proveedores externos y clientes:

Para facilitar las actividades de los proveedores externos y clientes, la Compañía brinda facilidades para el acceso a internet, sin embargo no puede realizar un control adecuado del acceso de los equipos que no pertenecen a Acotecnic, constituyéndose en una vulnerabilidad para la red de datos.

Es recomendable que se implemente una red dedicada con las restricciones del caso que facilite el acceso a los servicios de internet, pero que limite el acceso a la intranet. El uso de VLAN o de una conexión independiente podría facilitar estos accesos.

2 POLÍTICAS ADICIONALES

2.1 Política de protección de datos y privacidad de información personal.

Se debe definir una política respecto al uso y almacenamiento de información personal en recursos informáticos de la Compañía considerando el respeto y la privacidad de este tipo de datos.

Los miembros de la Compañía deben ser conscientes que no es potestad de la misma revisar los contenidos de la información personal, sin embargo puede utilizar esta información para comprobar el buen uso de los recursos asignados.

Debería limitarse al mínimo posible la cantidad de información personal que se almacene en los activos de procesamiento de datos de la Compañía.

Debe especificarse una ubicación determinada, de forma que la información personal quede fuera de los respaldos de información que el departamento de sistemas realice conforme se recomienda en la política de protección de la información.

2.2 Política para la gestión de la continuidad del negocio

Ante un incidente, es necesario que se establezcan los procedimientos adecuados para reducir al máximo el impacto de dicho incidente.

Se deben considerar los aspectos críticos del negocio. El restablecimiento y la continuidad de relaciones con empleados, proveedores y clientes deben restablecerse en el menor tiempo posible.

Entre los aspectos a considerarse tenemos: *(ítems tomados de la norma ISO/IEC 27002)*:

- Comprender los riesgos de la organización desde el punto de vista de vulnerabilidades e impacto, priorizando los de los procesos críticos del negocio.
- Identificar los activos implicados en los procesos críticos del negocio.
- Identificar los recursos financieros, organizacionales, técnicos y ambientales necesarios para la gestión de la seguridad de la información.

- Formular, documentar, probar y revisar continuamente planes de continuidad del negocio.
- Priorizar la seguridad del personal y la protección de las instalaciones.

2.2.1 Continuidad del Negocio y evaluación de riesgos:

Los eventos que puedan causar interrupciones a los procesos del negocio deben ser identificados, considerando la prioridad, impacto y consecuencias para la seguridad de la información. Se debe estimar la probabilidad de ocurrencia.

Es importante considerar los diferentes aspectos del riesgo para obtener una perspectiva completa, y de esta forma establecer de manera más exacta los procedimientos a seguir, determinando las pérdidas admisibles y los tiempos permisibles de interrupción para cada situación.

2.2.2 Implementación de planes de continuidad del negocio: Una vez creada la estrategia, la Gerencia deberá respaldarla y crear un plan de implementación.

Dentro de los procedimientos de emergencia, se deben incluir los procedimientos de recuperación, restauración de operaciones y disponibilidad de información en escalas de tiempo previamente establecidas.

Es importante considerar los tiempos establecidos dentro de las responsabilidades contraídas en contratos vigentes de la Compañía, ya que estos retrasos podrían causar pérdidas económicas debido a la imposición de multas.

La concientización y capacitación adecuada del personal, en cuanto a procedimientos, procesos de emergencia, gestión de crisis y responsabilidades en cada una de las etapas, asegurará que la continuidad del negocio sea restablecida en menor tiempo posible. Todos deben tener claro su rol y responsabilidades cuando sea necesario ejecutar un plan de emergencia.

Dentro de los planes de emergencia, se debe considerar una locación remota, que cuente con las seguridades necesarias, para almacenamiento de información sensible y activos necesarios para garantizar la continuidad de operaciones esenciales.

2.2.3 Pruebas, mantenimiento y reevaluación de los planes de continuidad:

Los planes de continuidad del negocio se deberían probar regularmente para asegurar su actualización y eficacia. Es necesario definir un calendario de mantenimiento que especifique cómo y cuándo se harán pruebas, así como el proceso para su mantenimiento.

Cada plan debe tener un responsable general, que se encargará de revisarlo, evaluarlo y de ser necesario modificarlo en base a nuevos requerimientos. Dichos cambios deben ser puestos a consideración de la Gerencia y posteriormente difundidos a los empleados, proveedores, clientes, etc., según sea conveniente para los fines de la Compañía.

Pruebas en papel, simulacros, y pruebas de recuperación técnica, en la oficina matriz, sucursales y locación alternativa remota, pueden servir para verificar la eficacia del plan.

Los resultados de la pruebas deben ser guardados y puesto en conocimiento de los miembros de la Compañía, poniendo énfasis en los resultados y las acciones tomadas en cuenta para mejorar el plan.

Factores que podrían modificar los planes de emergencia y continuidad de los mismos, podrían ser: cambio en el personal, cambios en la infraestructura física, cambios en la estrategia del negocio, cambios en los dispositivos y recursos, cambios en las relaciones con contratistas y proveedores, nuevos riesgos operativos y financieros, actualización y cambio de recursos informáticos, etc.

2.3 Política para el tratamiento de incidentes

2.3.1 Reporte de eventos y debilidades:

Reportar oportunamente, mediante los canales apropiados, cualquier evento o vulnerabilidad, garantiza que se tome una acción correctiva de forma oportuna.

Todas las personas involucradas en las actividades de la Compañía tienen la obligación de reportar cualquier evento en la seguridad o vulnerabilidad de información, lo más rápido posible.

Se deben establecer los canales de comunicación a ser utilizados y la persona de contacto que será la primera en atender el reporte, y la primera en actuar para minimizar el impacto de dicho evento en la continuidad del negocio.

Se debe establecer el procedimiento a seguir en caso de un evento de seguridad de la información, se deben registrar todos los detalles importantes. En ningún caso es recomendable que algún empleado no autorizado realice acciones correctivas por sí mismo, ya que esto podría agravar el problema.

Se deben establecer los métodos de retroalimentación para asegurarse de mantener informados a todos los miembros de la organización sobre el problema, una vez que se haya atendido y cerrado el tema.

Establecer el proceso disciplinario para empleados, contratista y terceros en caso que lleguen a comprometer la seguridad de la información y la continuidad del negocio, según la severidad del problema.

Entre los incidentes de información podemos encontrar *(ítems tomados de la norma ISO/IEC 27002)*:

- Pérdida de servicio, equipo o instalaciones.
- Sobrecargo o mal funcionamiento del sistema.
- Errores humanos.
- No conformidades con políticas o pautas.
- Cambios incontrolables en el sistema.
- Mal funcionamiento del software o hardware.
- Inserción de virus y códigos maliciosos.
- Violación de acceso.

Las acciones de emergencia deben ser documentadas a detalle y deben ser informadas a Gerencia de forma inmediata.

2.3.2 Aprendiendo de los incidentes:

Eventos ocurridos, pueden servir como medio ilustrativo en procesos de entrenamiento para la prevención de eventos de seguridad al interior de la Compañía, siempre y cuando se considere la confidencialidad adecuada para no comprometer la integridad de las personas, ni la continuidad del negocio.

Un proceso de mejora continua debe ser aplicado como resultado de los procedimientos de monitoreo, evaluación y gestión de seguridad de la información.

Es necesario determinar un mecanismo que permita identificar los tipos, volúmenes o costos de los incidentes de forma que puedan ser cuantificados y monitoreados, esto permitirá conocer los incidentes más repetitivos o los de mayor impacto.

2.3.3 Recolección de evidencias: Al momento de recopilar evidencias es conveniente que se considere lo siguiente *(ítems tomados de la norma ISO/IEC 27002)*:

- Las evidencias deben ser recopiladas de acuerdo a las normas y reglas internas de la Compañía y conforme establece la legislación vigente para que tengan validez jurídica.
- Que sean lo más completas posibles y que tengan la claridad y calidad necesario para efectos probatorios.
- Que sean guardas adecuadamente para precautelar la integridad de las mismas y sus respectivos respaldos, independientemente si éstas están guardadas en medios físicos y/o digitales. La cantidad de respaldos realizados debe estar claramente identificada.
- Si el incidente es considerado de suma gravedad para la continuidad del negocio, es aconsejable la participación de un abogado o la autoridad competente y que las pruebas sean protegidas adecuadamente para evitar cualquier eliminación o alteración accidental o intencional.

2.4 Política de seguridad física y del entorno.

2.4.1 Protección contra amenazas externas e internas.-

La Compañía cuenta con servicio contratado de vigilancia y sistemas de monitoreo con sensores de movimiento en distintas oficinas. Sin embargo es necesario mejorar la seguridad en el acceso a uno de los garajes, ya que por un daño esta puerta permanece abierta constituyendo un riesgo potencial para la seguridad física de la Compañía y su personal.

Se cuenta con área de recepción la que se encarga de permitir el acceso a la Compañía, no obstante, una vez que se ha ingresado y se ha pasado esta estación, no existe un control de acceso a las diferentes áreas de trabajo.

Se debería prohibir el ingreso a áreas restringidas, incluso a los empleados, sin la respectiva autorización. En el cuarto de equipos, se recomienda mejorar la solidez física y seguridad de la puerta.

Es necesario realizar pruebas periódicas de los sistemas de ingreso, alarmas, extintores de incendio y salidas de emergencia para garantizar su correcto funcionamiento. Se recomienda realizar simulacros para identificar potenciales riesgos, especialmente en caso de emergencia.

Materiales de fácil combustión deben permanecer alejados de los centros de respaldo de información.

De ser conveniente, la Compañía podrá disponer, para reuniones de trabajo con terceras personas y proveedores externos, de áreas de trabajo que cuenten con sistemas de seguridad, cámaras de vigilancia y redes de acceso a internet independientes de las redes que se utiliza para el trabajo cotidiano de la Compañía.

Todo personal que no pertenezca a la Compañía debería estar acompañado en caso de que sea necesario su ingreso a las diferentes áreas de la Compañía.

2.4.2 Seguridad de los equipos:

Se debe implementar un plan de mantenimiento preventivo periódico, que permitirá detectar amenazas y prevenir fallos en los sistemas de información.

Es aconsejable que se defina una política de buen uso de los recursos que la Compañía haya destinado para trabajos fuera de la oficina, y se cuente con los procesos de encriptación que protejan la información que se transporta fuera de las oficinas.

En caso de que se reutilice un equipo para otras actividades, es preciso que sea revisado previamente para asegurar su correcto funcionamiento y que no contenga información sensible o que no sea necesaria para las nuevas actividades que va a desempeñar.

3 MEJORAS TECNOLÓGICAS

3.1 Topología de la red actual.

Actualmente la red presenta un punto crítico en su topología. El servidor de virtualización es el único punto de enlace entre el ISP y la red de la Compañía. Este servidor realiza las funciones de firewall perimetral y Proxy. De presentarse alguna falla que deje fuera de servicio a este servidor, toda la red forzosamente saldría de servicio ya que no tendría otra conexión con el ISP.

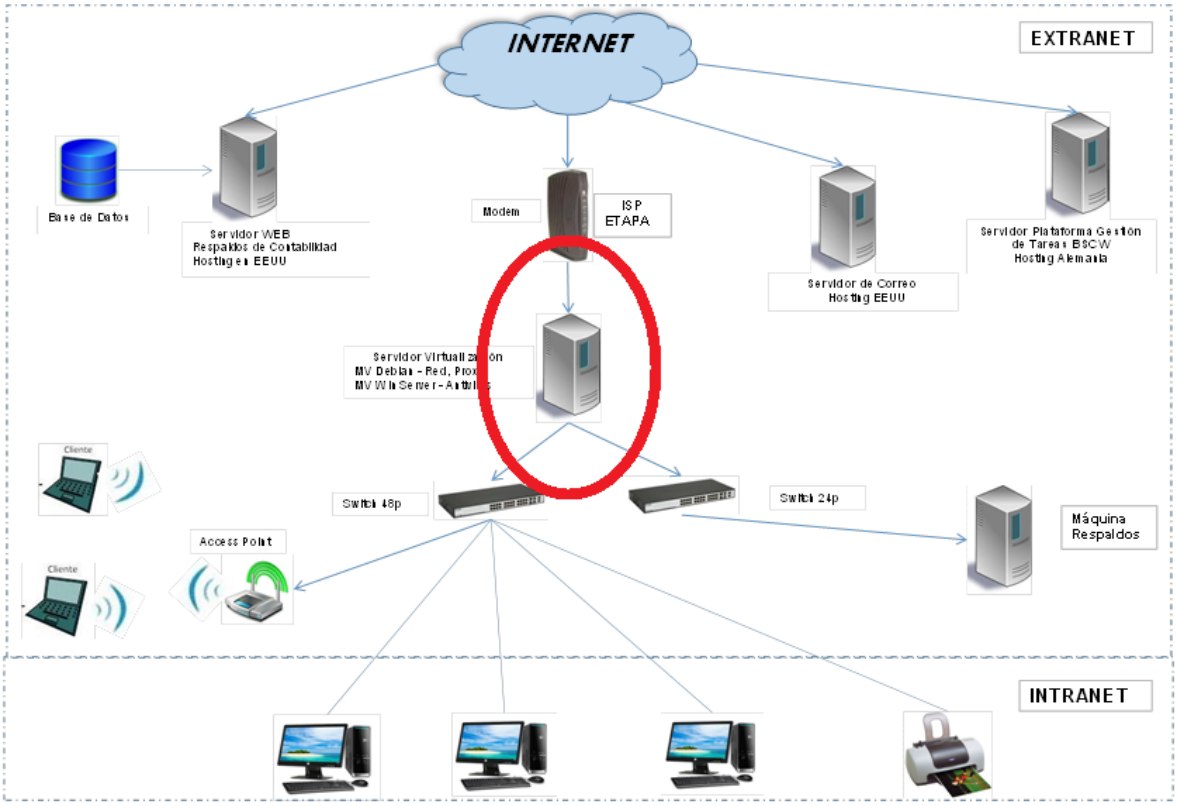


Figura: 5.1 Punto de vulnerabilidad en la red existente

3.2 Topología de la red mejorada.

Es recomendable cambiar los switch de capa 2 por switch de capa 3 que permitirán:

- Utilizar protocolos de enrutamiento
- Segmentar la red en redes VLANs
- Asignarles privilegios de acceso a cada VLAN
- Mayor interconectividad de equipos que los que permitiría un router.
- Mejor rendimiento de la red debido a la implementación de protocolos de transmisión.
- Gestión de ancho de banda.

Las redes VLAN permitirán agrupar usuarios de acuerdo a la actividad y función que realicen. Esta segmentación permitirá además gestionar el uso del ancho de banda de acuerdo a los privilegios previamente definidos.

Es recomendable la implementación de un equipo firewall cuyo funcionamiento esté independizado de la operación de los servidores.

Para validar el inicio de sesión en los equipos, se recomienda, además de la autentificación usuario-password, una autentificación por medio de la dirección MAC, especialmente en equipos con conexión WiFi.

En la figura 5.2 se muestra la propuesta de mejora física de la red.

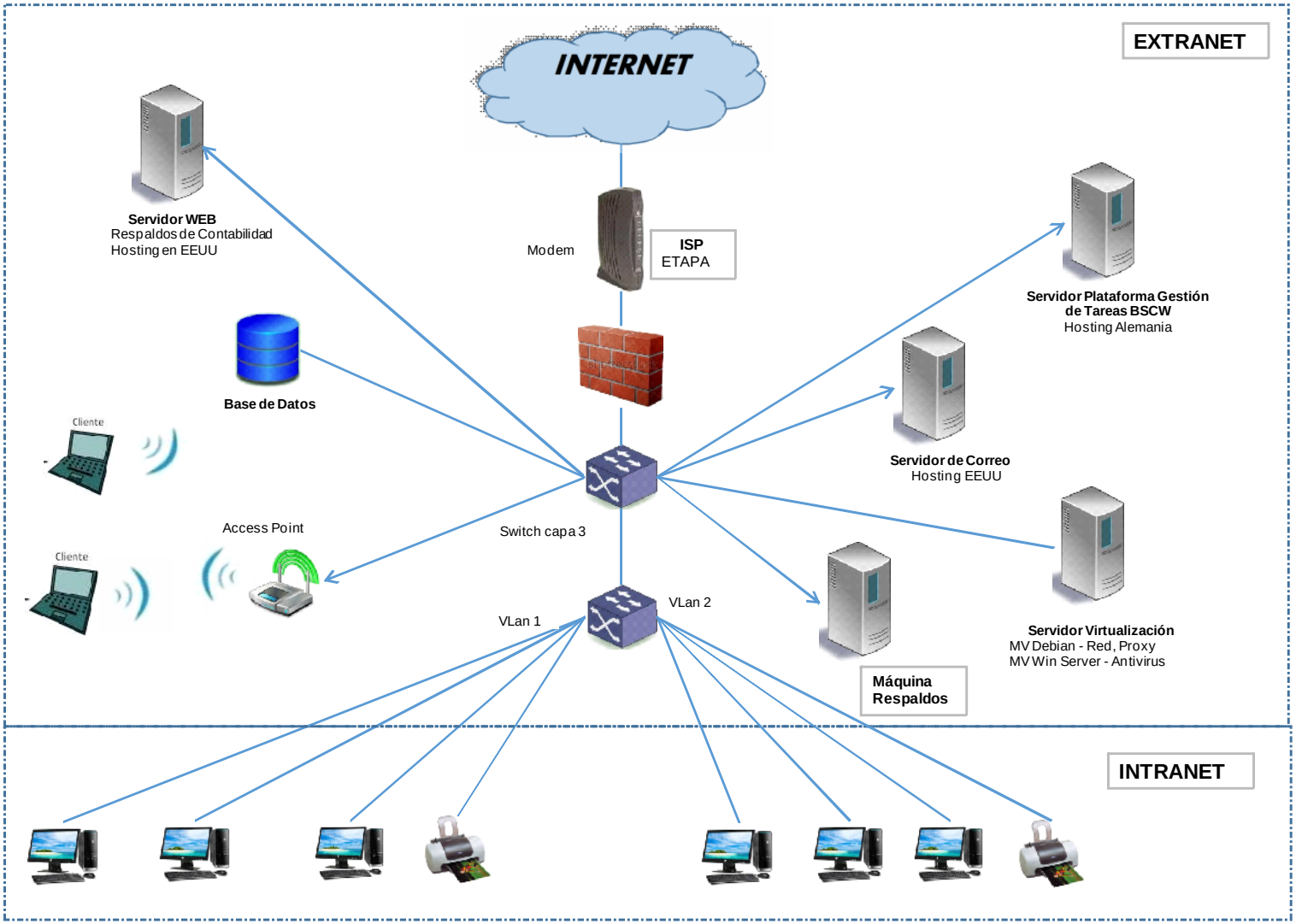


Figura: 5.2 Topología de red mejorada.

4. Estrategia de implementación del Sistema de Seguridad de la Información

4.1 Implementación a corto plazo.

Se deben atender los puntos más vulnerables para la seguridad de la información. La decisión sobre su implementación debe realizarse de manera inmediata (recomendable un plazo máximo de un mes).

Los controles a implementarse o mejorarse en esta etapa, son los relacionados a la toma de decisiones por parte de los Administradores para mejorar la seguridad de la información. Se debe coordinar internamente la creación de comisiones que se encarguen de definir las políticas a implementarse en base a las recomendaciones dadas al inicio de este capítulo.

Se debe definir a los responsables, al oficial de seguridad y los procedimientos para clasificar y proteger la información.

Se debe implementar los acuerdos de confidencialidad, buen uso de la información y no divulgación en el intercambio de información con proveedores externos, terceros y clientes, ya sea que esta se realice por medio de documentos en físico o en digital.

Se debe definir los procedimientos para eliminar o destruir la información en cualquier medio que ésta esté almacenada luego que no sea requerida, especialmente en dispositivos portátiles, unidades extraíbles o equipos que no sean de propiedad de la Compañía.

Se debe mejorar la seguridad física de la puerta de acceso del cuarto de equipos y la seguridad de las salidas y los equipos de emergencia.

Mejorar la seguridad en los puestos de trabajo, equipos desatendidos, escritorio y pantalla limpia.

Definir los controles a utilizarse en equipos portátiles y la política para realizar actividades de teletrabajo. Incluyendo las alternativas para encriptación de datos.

Estas decisiones, requieren escasa inversión económica. Se estima que se logrará alcanzar un porcentaje de cumplimiento del **52%.**

La estrategia planteada recomienda que se defina las políticas a implementarse y los controles que se aplicarán en cada una de ellas, se designen a los responsables y al oficial de la información, se mejore los procedimientos de manejo, custodia, almacenamiento y eliminación de la información, así como se establezca los acuerdos de confidencialidad, buen uso y no divulgación de la información, se incluyan estos controles en los procesos administrativos, especialmente en el manejo del recurso humano. Se mejore la seguridad física de las instalaciones.

Se puede observar en la Figura 5.3, que las decisiones de esta etapa mejorarán los índices de cumplimiento, especialmente en los dominios considerados más importantes.

Adicionalmente debido a la debilidad o escasos controles de la red actual, es necesario que se destine los recursos económicos mejorar la topología con la adquisición de equipos. Modificando la topología y configuración de los dispositivos.

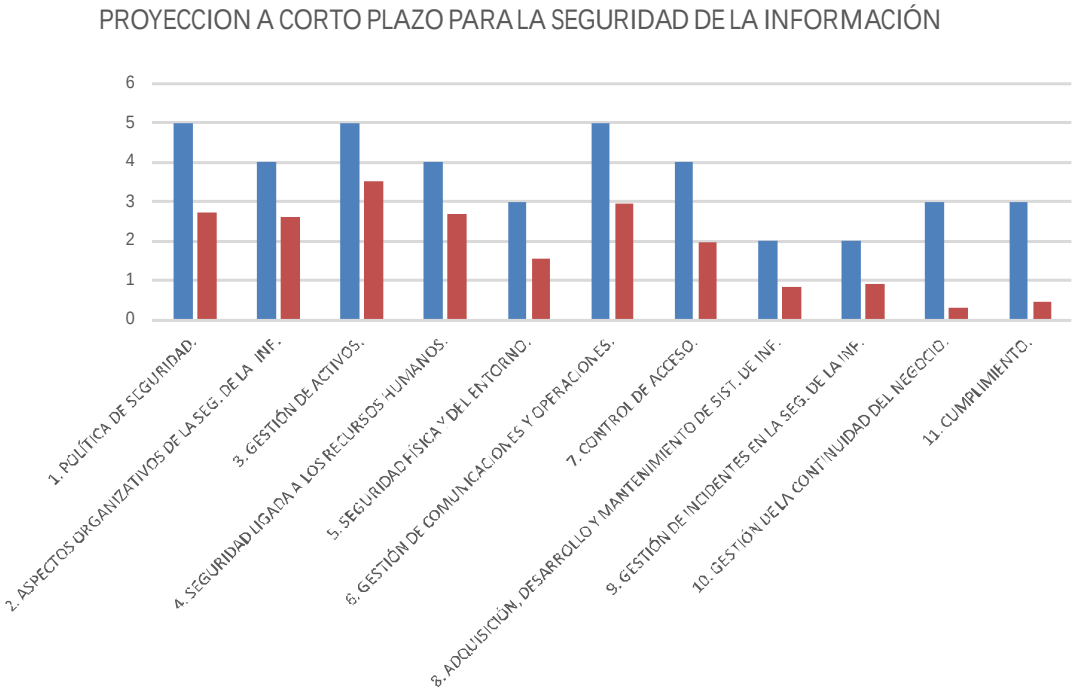


Figura: 5.3 Índices de cumplimientos estimados para la mejora a corto plazo

4.2 Implementación a mediano plazo.

Se debe atender los puntos que presenten una vulnerabilidad media y deben implementarse en un tiempo no mayor a 6 meses.

Se debe implementar las políticas de seguridad de la información, nombrar a los responsables, al oficial de la seguridad y los procedimientos a seguir.

Hay que reforzar la participación de todos los involucrados en el negocio, mediante la difusión de los procedimientos establecidos en las políticas de seguridad de la Compañía y su integración dentro de las actividades administrativas y operativas.

Se debe mejorar la topología de la red e implementar los controles que permitan gestionar el uso de los recursos y servicios de red. Se ha estimado que la mejora

en la topología de red requerirá una inversión económica de alrededor de 10000 USD.

Es necesario planificar la estrategia para la Gestión de la continuidad del negocio.

En esta etapa de implementación, se mejorarán los índices de cumplimiento de todos los dominios, especialmente los considerados más importantes, cómo se puede apreciar en la figura 5.4

El porcentaje de cumplimiento en este punto se estima que estará alrededor del

70%

En esta etapa se estima que la Compañía contará con las políticas y controles definidos, responsables asignados y procedimientos establecidos para el manejo e intercambio de la información, gestión de activos, especialmente los procedimientos para la devolución por parte de empleados y/o proveedores externos y terceros cuando culmine la relación laboral y comercial entre las partes. Todos los involucrados en las actividades de la Compañía estarían en conocimiento de las políticas y su obligación de cumplirlas. Es decir, que se tendría todas las reglas claras y definidas, la perspectiva de alcanzar un mayor nivel de cumplimiento, se centraría en el factor humano, en que se cumpla lo dispuesto.

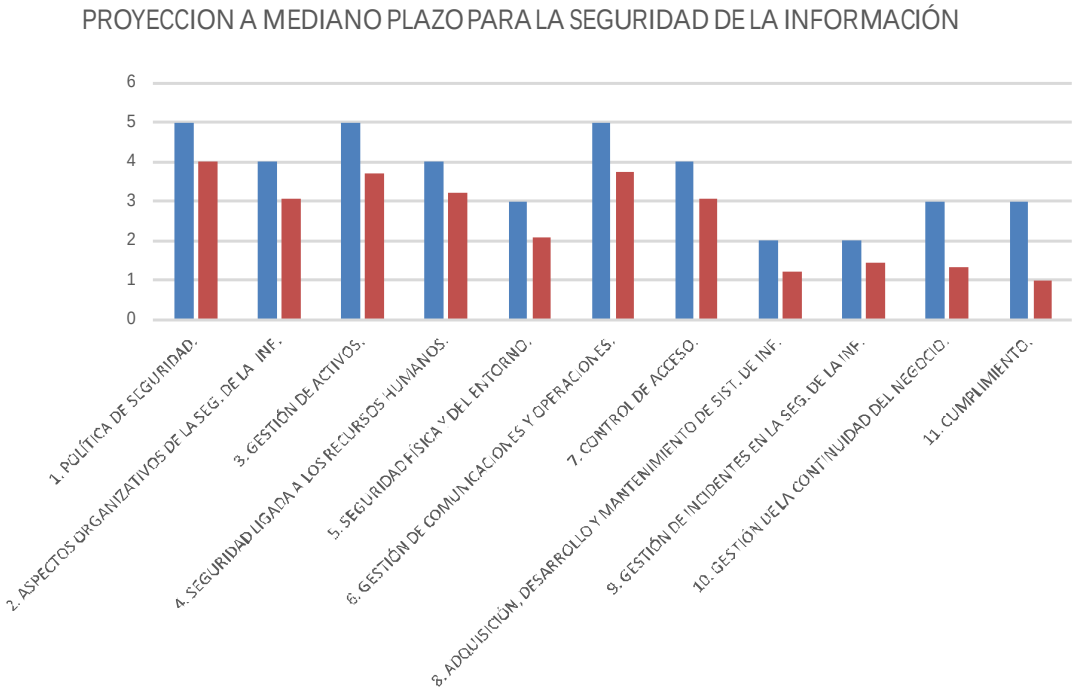


Figura: 5.4 Índices de cumplimientos estimados para la mejora a mediano plazo

4.3 Implementación a largo plazo.

Se debe atender los puntos que presenten menor vulnerabilidad y deben implementarse en un tiempo máximo de un año.

Esta etapa constituye la etapa de monitoreo de cumplimiento y depuración de los controles y procedimientos implementados.

Se estima que el índice de cumplimiento estaría alrededor del 87%. No se va a alcanzar el 100% de lo recomendado por la Norma ISO/IEC 27002, debido a que no se implementaran controles para procedimientos de auditorías, para el desarrollo o modificación de software o archivos del sistema operativo.

En la figura 5.5 se puede observar que se ha obtenido una mejora en todos los dominios de la seguridad de la información.

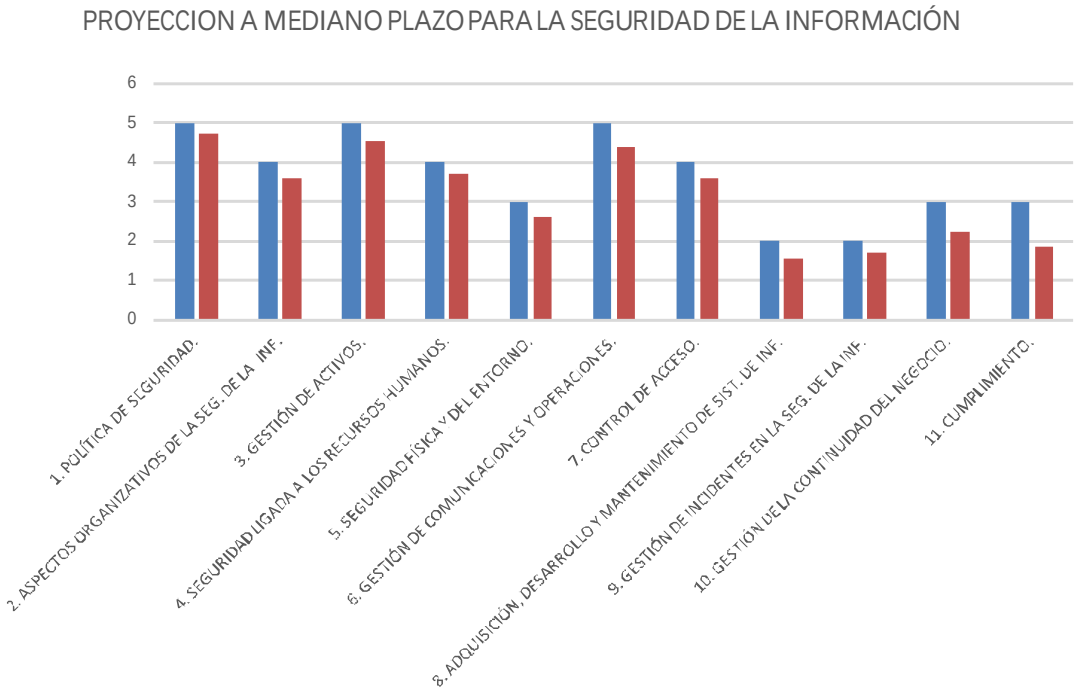


Figura: 5.4 Índices de cumplimientos estimados para la mejora a largo plazo

CAPÍTULO VI
Conclusiones y recomendaciones

6.1 Conclusiones

Al finalizar el presente estudio podemos concluir lo siguiente:

6.1.1 Estado de la Seguridad de la Información en la Compañía:

ACOTECNIC Cía. Ltda., no tiene procedimientos explícitos relacionados con la Seguridad de la Información, y se encuentran vulnerables ante amenazas; principalmente, relacionados al mal uso de recursos informáticos, la pérdida de información y la inseguridad de sus activos físicos.

Durante su vida institucional, la Compañía ha desarrollado varios proyectos en los cuales se ha generado información valiosa para el desarrollo de sus actividades comerciales; pero, debido a la falta de políticas definidas, han sido víctimas de pérdida, sustracción o mal uso de la información, sin tener una alternativa clara para proteger legalmente los derechos de propiedad, uso y confidencialidad de la información, así como asegurar la integridad y autenticidad de la información; requisitos necesarios para asegurar la continuidad del negocio.

Se realizan actividades de monitoreo, cuyos informes no son apropiadamente considerados para lograr un uso adecuado de los activos de red.

Las acciones que emprende la Compañía, en el campo de la seguridad de la información, generalmente son correctivas.

6.1.2 Riesgos existentes para el Sistema de Seguridad de la Información, en base a las recomendaciones dadas por la norma ISO/IEC 27002.

La inexistencia de políticas, procesos y procedimientos claramente definidos y adecuadamente comunicados a todos los involucrados en las actividades del negocio, constituye el principal riesgo al que está expuesta la Compañía.

En cuanto a la gestión de recursos humanos, se están implementando acciones correctivas mediante la imposición de sanciones económicas, sin embargo esto no es la decisión más conveniente, ya que la Compañía necesita disponibilidad de sus recursos.

En cuanto a la seguridad física de sus instalaciones, es necesario que se mejore la seguridad para el acceso a determinadas áreas y que se distribuyan de mejor forma la señalización y los equipos de seguridad.

La red existente es vulnerable ya que, por su topología, existe el riesgo de quedar inutilizable si se presenta alguna falla en el equipo de enlace y ataques orientados al robo, modificación, o borrado de información. Existe un solo servidor que realiza funciones de servidor de virtualización, proxy, firewall y único punto de enlace entre la intranet y el ISP.

En cuanto a la seguridad operacional y comunicaciones, es necesario que se establezcan privilegios de acceso en base a las funciones y actividades que ejecuta cada empleado. La implementación de VLANs permitirá una adecuada gestión de privilegios.

El uso de dispositivos portátiles, móviles y equipos inteligentes debe ser restringido, no en su uso, sino en los privilegios de acceso. El uso de una red dedicada puede facilitar y asegurar el uso de estos dispositivos con propósitos de comunicación.

Es necesario concientizar a todas las personas que intervienen en el negocio, sobre el uso adecuado de los recursos. Establecer derechos, obligaciones, y posibles sanciones ha demostrado ser un método disuasivo eficaz para modificar conductas especialmente las relacionadas al buen uso de los recursos de red.

No se cuenta con una estrategia y procedimientos a seguir en caso de ocurrir un evento en la seguridad de la información y los procedimientos para asegurar la continuidad del negocio.

Es necesario que todos los procesos, procedimientos y políticas que la Compañía considere necesarios, estén apegados a la normativa y legislación vigente, especialmente en el campo civil y laboral, de forma que se tenga un respaldo válido adecuado en caso de presentarse algún litigio de carácter legal.

6.1.3 Amenazas debido al factor humano

En la Gestión de Recursos Humanos es necesario que se defina una política adecuada que se pueda implementar antes, durante y al finalizar las relaciones laborales con sus candidatos y empleados, esto permitirá asegurar un uso correcto y confiable de sus activos, así como la recuperación de todos los activos de información con la integridad y disponibilidad adecuada.

6.1.4 Lineamientos base para determinar las políticas de seguridad más convenientes para la Compañía.

Considerando los factores de riesgo y las vulnerabilidades de la Compañía, en lo referente al manejo de la información por parte de empleados de planta, empleados ocasionales, proveedores externos y clientes, uso de los servicios de red, tratamiento de la información, almacenamiento y custodia de la misma, se recomienda la implementación, como mínimo, de las siguientes políticas:

- Política de clasificación de la información.
- Política de protección y acceso a la información.
- Política para el manejo de la información por parte de terceros y clientes.
- Política de destrucción de la información.
- Política de almacenamiento y recuperación de la información.
- Política para la Gestión de Recursos Humanos
- Política de control de accesos y uso de las TICs
- Política de uso apropiado de los servicios de red

Adicionalmente se pueden implementar las siguientes políticas, para complementar los escenarios que presentan menor vulnerabilidad a la seguridad de información al interior de la Compañía.

- Política de protección de datos y privacidad de información personal.
- Política para la gestión de la continuidad del negocio
- Política para el tratamiento de incidentes de seguridad
- Política de seguridad física.

6.2 Recomendaciones:

La implementación de nuevos sistemas está ligada a la inversión de recursos económicos, este es uno de los principales factores que frena la decisión de implementarlas.

Durante el desarrollo del presente proyecto se ha identificado varios controles, recomendados por la norma ISO/IEC 27002, que se pueden asociar a procedimientos de carácter administrativo y procedimientos de carácter técnico con mínimos costo económico.

- **Procedimientos de carácter administrativo:** No requieren de una inversión económica mayor, más bien se trata de decisiones respaldadas por la Alta Gerencia que modifiquen algunos procesos y procedimientos internos.

- **Procedimientos de carácter técnico:** Se refieren a procesos operativos, que requieren una inversión económica en el área técnica, que garanticen la correcta operación. Dentro de estos procedimientos, está la mejora en la topología de la red.

Se recomienda que se implementen los procesos de carácter administrativo, ya que estos serán una herramienta importante para modificar la conducta de las personas, reduciendo significativamente la posibilidad de ocurrencia de eventos que afecten a la seguridad de la información y a la continuidad del negocio.

Independientemente del costo, es sumamente importante que se realicen los correctivos necesarios en la edificación, especialmente lo relacionado con la seguridad de las puertas y distribución de equipos de emergencia, con el fin de precautelar la seguridad e integridad física del personal.

Se recomienda que se realice el cambio en la topología de red, lo que permitirá una gestión más adecuada de los recursos de red y la segregación de usuarios en base a la función que ejecuten dentro de la Compañía. Sin embargo, de considerarse que no es conveniente esta inversión, se recomienda implementar un servidor espejo de forma que si falla el servidor principal, entre en operación el servidor espejo (de respaldo), reduciendo significativamente el tiempo de respuesta para restablecer los servicios de red.

Bibliografía y Fuentes de Información

[1] Fundación Wikipedia Inc, Serie de normas ISO/IEC 27000, agosto.20.2013, http://es.wikipedia.org/wiki/ISO/IEC_27000-series

[2] IEC – Webstore de la Comisión Electrotécnica Internacional, Preview de las normas ISO serie 27000 publicadas - versión original - incluyen Abstract – Introducción e Indice, 2013, http://webstore.iec.ch

[3] Agustín López Neira & Javier Ruiz Spohr – Portal en español de la norma ISO 2700, Sistema de Gestión de la Seguridad de la Información, http://www.iso27000.es/sgsi.html

[4] Agustín López Neira & Javier Ruiz Spohr – Portal en español de la norma ISO 2700, Serie ISO 27000, http://www.iso27000.es/sgsi.html

[5] The ISO 27000 Directory- , A Short History of the ISO 27000 Standards, 2007, http://www.27000.org/thepast.htm

[6] The ISO 27000 Directory- , An Introduction to ISO 27001, ISO 27002....ISO 27008, 2013, http://www.27000.org/thepast.htm

[7] Revista Ekos Negocios, Roberto Chávez, ERS (Enterprise RiskServices), Noticias empresariales Ecuador: “Deloitte explicó a entidades públicas los lineamientos para la ejecución de la norma de seguridad 2014”, Noviembre.29.2013, http://www.ekosnegocios.com/negocios/m/verArticulo.aspx?idart=2703&c=1

[8] The British StandardsInstitution - España, Seguridad de la Información ISO 27001 – Auditoria y Certificación, 2013, http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion

[9] Instituto Ecuatoriano de Normalización - Subcomité Técnico de "Tecnologías de la Información”, Normas propuestas para el proyecto de Regulación de las

TIC's, Normas de Seguridad, 2011, http://www.inen.gob.ec/index.php?option=com_content&view=article&id=163&Itemid=154

[10] Instituto Ecuatoriano de Normalización - Normas Técnicas Ecuatorianas NTE INEN ISO, ISO/IEC aprobadas por el Subcomité Técnico de Tecnologías de la Información, 2012, http://www.inen.gob.ec/images/pdf/normaliza/NTE%20aprobadas%20SCT%20TIC%202012.pdf

[11] Registro Oficial de la República de Ecuador, No. 699 del 09 de mayo de 2012, Ministerio de Industrias y Productividad, Subsecretaría de la Calidad, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27000, NTE-INEN-ISO/IEC 27003, NTE-INEN-ISO/IEC 27004, NTE-INEN-ISO/IEC 27005.

[12] Registro Oficial de la República de Ecuador, No. 491 del 14 de julio de 2011, Ministerio de Industrias y Productividad, Subsecretaría de Industrias, Productividad e Innovación Tecnológica, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27001.

[13] Registro Oficial de la República de Ecuador, No. 596 del 22 de mayo de 2009, Instituto Ecuatoriano de Normalización, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27002.

[14] Registro Oficial de la República de Ecuador, No. 654 del 06 de marzo de 2012, Ministerio de Industrias y Productividad, Subsecretaría de la Calidad, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27006.

[15] Registro Oficial de la República de Ecuador, No. 88 del 19 de septiembre de 2013 (segundo suplemento), Función Ejecutiva de la República del Ecuador, Acuerdo Ejecutivo No. 166 del 19 de septiembre de 2013, Secretaría Nacional de la Administración Pública, Disposición a las Entidades de la Administración Pública Central, Institucional y que dependan de la Función Judicial el uso obligatorio de las Normas NTE INEN ISO/IEC 27000. Implementación del EGSI.

Índice de Figuras

Capítulo II

Capítulo III

Capítulo IV

Índice de Tablas

Capítulo III

Capítulo IV

Glosario de Conceptos Técnicos

A

Ataques de Monitorización [32]

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro. El monitoreo se realiza mediante varias formas:

1.- Shoulder Surfing:

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente.

2.- Decoy:

Son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logueo y el usuario desprevenido lo hace.

3.- Scanning (Búsqueda)**:**

El escaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (escanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

[32] Fuente: http://www.segu-info.com.ar/ataques/tipos.htm. Título: SeguInfo Seguridad de la Información. Autor: Cristian Borghello. Fecha de ingreso: Marzo 2015

- TCP Connect Scanning

  Esta es la forma básica del escaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

- TCP SYN Scanning

  La técnica TCP SYN Scanning, implementa un escaneo de "media-apertura", dado que nunca se abre una sesión TCP completa. Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

- TCP FIN Scanning– Stealth Port Scanning

  Este tipo de escaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión. Es posible aplicarlos en algunos sistemas Unix.

- Fragmentation Scanning

  Esta no es una nueva técnica de escaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

4.- Eavesdropping–PacketSniffing

Esto se realiza con packet sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo router o a un gateway de internet.

Un sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a la computadora donde está instalado el sniffer.

5.- Snooping–Downloading

En este método, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos copia de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

Ataques de Autenticación [33]

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo, tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

1.- Spoofing-Looping

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.

[33] Fuente: http://www.segu-info.com.ar/ataques/tipos.htm. Título: SeguInfo Seguridad de la Información. Autor: Cristian Borghello. Fecha de ingreso: Marzo 2015

2.- Spoofing

Son ataques sobre protolocos. Entre ellos están:

- IP Spoofing

  Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso.

- Web Spoofing

  En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc.

- IP Splicing–Hijacking

  Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

- Utilización de Back Doors

  Las puertas traseras son trozos de código en un programa que permiten saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo.

- Utilización de Exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

- Obtención de Passwords

  Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados, mediante algún tiempo de prueba y error.

  - ✓ Uso de Diccionarios

    Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha contraseña en pruebas de fuerza bruta.

Ataques de Modificación - Daño

- Tampering o Data Diddling

  Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima incluyendo eliminación de archivos; obteniendo derechos de administrador o supervisor. Incluso, si no hubo intenciones de "bajar" el sistema por parte del atacante; el Administrador posiblemente necesite darlo de baja por algún tiempo hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada. En ocasiones se remplazan las versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.).

- Borrado de Huellas

  Las huellas son todas las tareas y acciones que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo. Los archivos Logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

- Ataques Mediante Java Applets

  Los Applets de Java son códigos ejecutables y como tal, susceptibles de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los Applets (imposibilidad de trabajar con archivos a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos especializados en descubrir fallas de seguridad en las implementaciones de las Máquinas Virtuales Java.

- Ataques Mediante JavaScript y VBScript

  JavaScript (de la empresa Netscape®) y VBScript (de Microsoft®) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Los programas realizados son interpretados por el navegador. Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.

- Ataques Mediante ActiveX

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft®. Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft® a Java.

ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales.

La filosofía ActiveX es que las Autoridades de Certificación se fían de la palabra del programador del control. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar.

- Vulnerabilidades en los Navegadores

En los navegadores suelen fallar las tecnologías con las que se implementan, como por ejemplo los "Buffer Overflow".

Los "Buffer Overflows" consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones. Un conocimiento adecuado del lenguaje Assembler es suficiente para este tipo de ataques.

Por ejemplo:

www.servidor.com/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

devuelve el directorio de la unidad c: del servidor deseado.

C

Código malicioso

También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. En inglés se lo llama malware: malicious software e incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables. [34]

Código móvil

Es el software de transferencia entre sistemas, por ejemplo, transferidas a través de una red o mediante una unidad flash USB, y ejecutado en un sistema local sin necesidad de instalación o ejecución explícita por parte del beneficiario. [35]

D

Denial of Service (DoS)

Los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

[34] Fuente: http://es.wikipedia.org/wiki/Malware
[35] Fuente: http://es.scribd.com/doc/39430270/codigo-movil#scribd

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.
2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un "crash" del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
5. El administrador del sistema tiene un proceso que no puede "matar" en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DoS deteniendo los servicios.

- Jamming o Flooding

  El atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

- SynFlood

  El cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el host responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

- ConnectionFlood

  Un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del SYN Flood) para mantener fuera de servicio el servidor.

- Net Flood

  En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil.

  En el caso de Net Flooding el atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir.

- LandAttack

  Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows©.

  El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al NetBIOS 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.

- Smurf o Broadcast Storm

  Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones Broad Cast para, a continuación,

mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima).

- OOB, Supernuke o Winnuke

Un ataque característico, y quizás el más común, de los equipos con Windows© es el Nuke, que hace que los equipos que escuchan por el puerto NetBIOS sobre TCP/UDP 137 a 139, queden fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados.

Generalmente se envían fragmentos de paquetes Out Of Band, que la máquina víctima detecta como inválidos pasando a un estado inestable. OOB es el término normal, pero realmente consiste en configurar el bit Urgente (URG) en los indicadores del encabezamiento TCP, lo que significa que este bit es válido.

- Teardrop I y II-Newtear-Bonk-Boink

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT© 4.0 de Microsoft® es especialmente vulnerable a este ataque. Aunque existen Patchs (parches) que pueden aplicarse para solucionar el problema, muchas organizaciones no lo hacen, y las consecuencias pueden ser devastadoras.

- E–Mail Bombing–Spamming

El e-mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario.

El Spamming, en cambio se refiere a enviar un e–mail a miles de usuarios, hayan estos solicitado el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos.

F

Fiabilidad.- Probabilidad de que un sistema, aparato o dispositivo cumpla una determinada función bajo ciertas condiciones durante un tiempo determinado. [36]

Ingeniería Social

Es un método basado en el engaño y la persuasión que puede llevarse a cabo a través de canales tecnológicos o bien en persona, y que se utiliza para obtener información significativa o lograr que la víctima realice un determinado acto. Un ejemplo de la aplicación de esta técnica es el phishing. [37]

Ingeniería Social Inversa - ISI

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovecha esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

P

Pishing

Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como

[36] Fuente: http://es.wikipedia.org/wiki/Fiabilidad. Fecha de ingreso, Enero 2015
[37] Fuente: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12. Título: Universidad Nacional de Luján – Buenos Aires Argentina. Fecha de ingreso: Febrero 2015

phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. [38]

T

Trashing

Es la acción de recolectar información a partir de material descartado, comúnmente con la finalidad de obtener datos que sirvan como información para cometer fraudes.

Si la información se recolecta de los cestos de papeles (papeles, diskettes, discos compactos) se habla de trashing físico. Cuando el atacante procura conseguir información revisando los archivos que puedan estar en la computadora (papelera de reciclaje, historial de navegación, o los archivos que almacenan cookies), se denomina trashing lógico. [39]

V

Vulnerabilidad: Debilidad en un activo que lo hace susceptible de ser atacado.

[38] Autor: Ed Skoudis. Phone phishing: The role of VoIP in phishing attacks. 13 de junio de 2006. Fecha de ingreso: Enero 2015

[39] Fuente: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12. Título: Universidad Nacional de Luján – Buenos Aires Argentina. Fecha de ingreso: Febrero 2015

ANEXOS

Inventario Detallado de Activos

ANEXO DE INVENTARIO DE ACTIVOS - COMPUTADORAS											
ITEM	**EQUIPO**	**TIPO**	**FABRICANTE**	**PROCESADOR**	**VELOCIDAD (GHZ)**	**MEMORIA (GB)**	**DISCO (GB)**	**MONITOR**	**PANTALLA**	**RED**	**S.O**
035	Equipo $_{1}$	PORTATIL	AMD	ATHLON II DUAL CORE	2	2	320	HP	14	LAN / WLAN	WIN 7 ULTIMATE
034	Equipo $_{2}$	PORTATIL	AMD	TURION II	2.5	4	500	HP	17	LAN / WLAN	WIN 7 HOME
006	Equipo $_{3}$	PORTATIL	INTEL	CORE 2 DUO	2	4	160	DELL	17	LAN / WLAN	WIN 7 PROFESSIONAL
037	Equipo $_{4}$	CPU	INTEL	CORE 2 QUAD	2.66	8	320	LG	19	LAN / WLAN	WIN 7 PROFESSIONAL
005	Equipo $_{5}$	PORTATIL	INTEL	DUAL CORE PENTIUM	2.2	2	320	TOSHIBA	15	LAN / WLAN	WIN 7 HOME
080	Equipo $_{6}$	PORTATIL	INTEL	I3	2.2	4	500	DELL	14	LAN / WLAN	WIN 7 ULTIMATE
102	Equipo $_{7}$	PORTATIL	INTEL	I5	2,50	8	1000	TOSHIBA	15	LAN / WLAN	WIN 8.1 PRO
050	Equipo $_{8}$	CPU	INTEL	I7	3.4	16	1500	LG	22	LAN	WIN 7 ULTIMATE
028	Equipo $_{9}$	PORTATIL	INTEL	PENTIUM	1.7	0.5	60	HP	15	LAN / WLAN	WIN XP PROFESSIONAL
059	Equipo $_{10}$	PORTATIL	INTEL	TURION II	2.5	4	500	HP	17	LAN / WLAN	WIN 7 HOME
090	Equipo $_{11}$	CPU	INTEL	XEON QUAD CORE	3,10	8	2000	N/A	N/A	LAN / WLAN	LINUX DEBIAN
096	Equipo $_{12}$	PORTATIL	MAC	CORE 2 DUO	2,66	4	320	MAC	13	LAN / WLAN	MAC OS 10,6
098	Equipo $_{13}$	PORTATIL	MAC	I5	2,50	4	500	MAC	13	LAN/WLAN	MAC MAVERIKS
099	Equipo $_{14}$	PORTATIL	MAC	I7	3,40	8	250	MAC	15	WLAN	WIN 7 ULTIMATE
054	Equipo $_{15}$	IMAC	INTEL	I7	2.93	8	1000	MAC	27	LAN	LION 10.6.8

Normas Serie ISO 27000

Estado actual de la Normativa a nivel Internacional y Nacional

Ing. Darwin S. Lanche C.
Maestría en Telemática
Universidad de Cuenca
Azuay, Ecuador
dlanchec@yahoo.es
Diciembre de 2013

Abstract - El presente documento constituye el "Estado del Arte" de la normativa ISO/IEC serie 27000 aplicable a los Sistemas de Gestión de la Seguridad de la Información. El documento está estructurado de la siguiente forma: En la introducción, en forma general, se hace referencia a la importancia de contar con un sistema de gestión de seguridad de la información (SGSI) y la familia de estándares ISO dedicadas a esta tarea, así como las versiones, en inglés o español disponibles. En la sección II se enumeran todas las normas que componen la familia ISO 27000. En la sección III se hace un análisis de cada norma, especialmente al área a la que está dedicada, el estado de publicación y si se dispone o no de una versión en español. En la sección IV se resume el proceso a seguir para obtener la certificación ISO 27001. Culminando con la Sección V en donde se hace una revisión del estado actual de la normativa en el Ecuador y los planes de gobierno respecto a la implementación de SGSI en las Instituciones de la Administración Pública o que están relacionadas a la Función Ejecutiva.

Palabras Clave: Seguridad informática, SGSI, ISO 27000, Certificación ISO 27001.

Introducción

La información tiene importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la organización.

Las normas que componen la familia de series ISO 27000, son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Es una recopilación de las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar, mantener y mejorar los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Las versiones originales de las normas ISO, vienen en idioma inglés, sin embargo algunas normas han sido traducidas al español y se pueden encontrar en la página web de la Asociación Española de Normalización y Certificación AENOR en www.aenor.es, en otros casos, algunas normas han sido traducidas al español por entidades nacionales, dependiendo de la necesidad de cada País. Esto explica la aparición de publicaciones con fechas diferentes a las versiones originales en inglés. Muchas de estas traducciones han sido realizadas para propósitos de interés nacional del País que realiza la traducción.

Las normas ISO Serie 27000 no son de libre distribución y se pueden comprar en formato PDF o en CD o DVD en el sitio web oficial de la ISO www.iso.org Es posible acceder a una visualización del contenido (índice) de las normas que ya han sido publicadas como estándares internacionales por la ISO, en el webstore del IEC webstore.iec.ch

Normas de la Serie ISO/IEC 27000

Algunas normas de esta serie se encuentran en proceso de preparación.

Las normas que forman parte de esta serie son:

ISO/IEC 27000 - Información general y vocabulario para los SGSI.

ISO/IEC 27001 - Requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI.

ISO/IEC 27002 - Es un código de las mejores prácticas para la Gestión de Seguridad de la Información.

ISO/IEC 27003 – Guía de aspectos necesarios para el diseño e implementación de un SGSI.

ISO/IEC 27004 - Desarrollo y uso de medidas para la evaluación de la eficacia de un SGSI.

ISO/IEC 27005 - Gestión de riesgos de seguridad de información.

ISO/IEC 27006 - Requisitos para los organismos que realizan la auditoría y certificación de SGSI.

ISO/IEC 27007 - Guía para las organizaciones que se encargan de auditar SGSIs.

ISO/IEC 27008 - Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

ISO/IEC 27010 - Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.

ISO/IEC 27011 - Guía para la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones.

ISO/IEC 27013 - Guía de implementación integrada de ISO/IEC 27001 y de ISO/IEC 20000-1 (gestión de servicios TI).

ISO/IEC 27014 - Guía para la Administración Corporativa de la seguridad de la información.

ISO/IEC 27015 - Guía para la implementación y gestión de la seguridad de la información en el sector financiero y de seguros.

ISO/IEC 27016 - Valoración de los aspectos financieros de la seguridad de la información.

ISO/IEC 27017 - Guía de seguridad para Cloud Computing.

ISO/IEC 27018 - Código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

ISO/IEC 27019 - Guía para la gestión de seguridad de la información aplicada a los sistemas de administración, control y automatización que se utiliza en la industria de servicios públicos de energía.

ISO/IEC 27031 - Describe los conceptos y principios de la tecnología de información y comunicación (TIC) y la preparación de una organización para mantener la continuidad del negocio.

ISO/IEC 27032 - Guía de orientación para la mejora del estado de seguridad cibernética.

ISO/IEC 27033 - Parcialmente desarrollada, está dedicada a la Seguridad en Redes, consta de siete partes.

27033-1 Conceptos generales

27033-2 Directrices de diseño e implementación de seguridad en redes.

27033-3 Escenarios de referencia de redes.

27033-4 Aseguramiento de las comunicaciones entre redes mediante gateways de seguridad.

27033-5 Aseguramiento de comunicaciones mediante VPNs.

27033-6 Convergencia IP.

27033-7 Redes inalámbricas.

ISO/IEC 27034 - Dedicada a la seguridad en aplicaciones informáticas, consta de cinco partes.

27034-1 Conceptos generales.

27034-2 Marco normativo de la organización.

27034-3 Proceso de gestión de seguridad en aplicaciones.

27034-4 Validación de la seguridad en aplicaciones.

27034-5 Estructura de datos de protocolos y controles de seguridad de aplicaciones.

ISO/IEC 27035 - Guía sobre la gestión de incidentes de seguridad en la información.

ISO/IEC 27036 - Guía para la seguridad en las relaciones con proveedores, consta de cuatro partes.

27036-1 Visión general y conceptos.

27036-2 Requisitos comunes.

27036-3 Seguridad en la cadena de suministro TIC.

27036-4 Seguridad en Outsourcing (externalización de servicios).

ISO/IEC 27037 - Guía que proporciona las directrices para las actividades específicas en el manejo de la evidencia digital: identificación, recolección, consolidación y preservación del potencial de la evidencia digital que puede ser de valor probatorio.

ISO/IEC 27038 - Guía de especificación para seguridad en la redacción digital.

ISO/IEC 27039 - Guía para la selección, despliegue y operatividad de sistemas de detección y prevención de intrusión (IDS/IPS).

ISO/IEC 27040 - Guía para la seguridad en medios de almacenamiento.

ISO/IEC 27041 - Guía para garantizar la idoneidad y adecuación de los métodos de investigación.

ISO/IEC 27042 - Guía con directrices para el análisis e interpretación de las evidencias digitales.

ISO/IEC 27043 - Desarrollará principios y procesos de investigación.

ISO/IEC 27044 - Gestión de eventos y de la seguridad de la información.

ISO/IEC 27799 - Directrices para apoyar la interpretación y aplicación de los SGSI en el sector Salud.

Descripción Individual De Las Normas ISO/IEC Serie 27000

ISO/IEC 27000 - Proporciona una visión general de las normas que componen la serie ISO 27000.

Contiene información general y vocabulario para los SGSI.

Versiones en inglés: Fue publicada como estándar internacional en Mayo de 2009, la segunda y última versión se publicó en Diciembre de 2012. Está disponible de forma gratuita en standards.iso.org/ittf/PubliclyAvailableStandards

Versiones en español: Traducida por Uruguay bajo el nombre de UNIT-ISO/IEC 27000

ISO/IEC 27001 - Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. Es la norma más importante de la familia. Es la certificación que deben obtener las organizaciones. La versión más reciente pone énfasis en la medición y evaluación del SGSI implementado en una organización. En su Anexo A, se enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSIs. A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Versión en inglés: Fue publicada como estándar internacional en octubre de 2005, la versión actualizada (segunda edición) fue publicada en Septiembre de 2013.

Versión en español: Traducida para España bajo el nombre UNE-ISO/IEC 27001:2007, Colombia bajo el nombre NTC-ISO-IEC 27001, Venezuela bajo el nombre Fondonorma ISO/IEC 27001, Argentina bajo el nombre IRAM-ISO IEC 27001, Chile bajo el nombre NCh-ISO27001, México bajo el nombre NMX-I-041/02-NYCE, Uruguay bajo el nombre UNIT-ISO/IEC 27001.

ISO/IEC 27002 - Es un código de las mejores prácticas para la Gestión de Seguridad de la Información. Básicamente describe cientos de potenciales directrices y mecanismos de control, que pueden ser implementadas, en teoría, con sujeción a los lineamientos proporcionados en la norma ISO 27001. **Versión en inglés:** Publicada originalmente como un cambio de nombre de la norma ISO 17799 en julio de 2005 y recibió su nombre oficial ISO 27002 en julio de 2007. La última versión de esta norma (segunda edición) se publicó en Septiembre de 2013.

Versión en español: Traducida para: España UNE-ISO/IEC 27002:2009, **Colombia** NTC-ISO-IEC 27002, **Venezuela** Fondonorma ISO/IEC 27002, **Argentina** IRAM-ISO-IEC 27002, **Chile** NCh-ISO27002, **Uruguay** UNIT-ISO/IEC 27002, **Perú** como ISO 17799.

ISO/IEC 27003 – Guía de aspectos necesarios para el diseño e implementación de un SGSI. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

Versión en inglés: Publicada en Febrero de 2010.

Versión en español: Traducida para **Uruguay** UNIT-ISO/IEC 27003.

ISO/IEC 27004 - Proporciona orientación sobre el desarrollo y el uso de medidas y de medición para la evaluación de la eficacia de un SGSI aplicadas y los controles, tal como se especifica en la norma ISO 27001 y las métricas, incluidos los controles de ISO27002. Brinda recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.

Versión en inglés: Publicada en Diciembre del 2009.

Versión en español: Traducida para **Argentina** IRAM-ISO-IEC 27004, **Uruguay** UNIT-ISO/IEC 27004.

ISO/IEC 27005 - La norma proporciona las directrices para la gestión de riesgos de seguridad de la información en una organización, apoyando específicamente los requisitos de un SGSI que se define en la norma ISO 27001. Es aplicable a todo tipo de organización. No proporciona o recomienda una metodología específica, ya que esto dependerá de una serie de factores, tales como el alcance real del SGSI, tamaño o el sector comercial de la empresa.

Versión en inglés: Publicada en Junio de 2008, la última versión (segunda versión) fue publicada en Junio de 2011.

Versión en español: Traducida para **México** NMX-I-041/05-NYCE, **Chile** NCh-ISO27005, **Uruguay** UNIT-ISO/IEC 27005, **Colombia** NTC-ISO-IEC 27005.

ISO/IEC 27006 - Requisitos para los organismos que realizan la auditoría y certificación de SGSI. Esta norma ofrece las directrices para la acreditación de las organizaciones que ofrecen la certificación y el registro con respecto a un SGSI. Esta norma está destinado a ser utilizado en conjunción con otras normas ISO: ISO 27001, ISO 17021 (Requisitos para los organismos que realizan la auditoría y la certificación de sistemas

de gestión) e ISO 19011 (Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental).

Versión en inglés: Publicada como norma internacional en 2007, la última versión (segunda edición) fue publicada en Diciembre de 2011.

Versión en español: Traducida para **México** NMX-I-041/06-NYCE, **Chile** NCh-ISO27001.

ISO/IEC 27007 - Guía para las organizaciones que se encargan de auditar SGSIs.

Es aplicable a aquellas organizaciones que necesitan comprender o realizar auditorías internas o externas de un SGSI o para gestionar un programa de auditoría SGSI.

Versión en inglés: Publicada en Noviembre de 2011.

Versión en español: No se tiene registro de versiones traducidas.

ISO/IEC 27008 - Proporciona orientación sobre la revisión de la implementación y operación de los controles, incluyendo la comprobación del cumplimiento técnico del sistema de información, de conformidad con las normas establecidas de seguridad de información de una organización. Es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro que llevan a cabo revisiones de seguridad de la información y los controles de conformidad técnica.

Versión en inglés: Publicada en Octubre de 2011.

Versión en español: No se tiene registro de versiones traducidas.

ISO/IEC 27010 - Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. Es aplicable a todas las formas de intercambio y difusión de información sensible, entre entidades tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores.

En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización, o de la infraestructura crítica de los estados y naciones.

Proporciona una orientación para el inicio, implementación, mantenimiento y mejora continua de la seguridad de la información en las comunicaciones interinstitucionales e intersectoriales.

Versión en inglés: Publicada en Octubre de 2012.

Versión en español: No se tiene registro de versiones traducidas.

ISO/IEC 27011 - Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones. Está publicada también como norma ITU-T X.1051.

Tiene como objetivo definir directrices que permitan a las organizaciones de telecomunicaciones satisfacer las necesidades de confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad dentro de la gestión de seguridad de la información.

Versión en inglés: Publicada en Diciembre de 2008.

Versión en español: No se tiene registro de versiones traducidas.

ISO/IEC 27013 - Es una guía de implementación integrada de ISO/IEC 27001 y de ISO/IEC 20000-1 (gestión de servicios TI) para las organizaciones que pretendan:

Implementar la norma ISO/IEC 27001 teniendo ya implementada la norma ISO/IEC 20000-1, o viceversa.

Aplicar las normas ISO/IEC 27001 e ISO/IEC 20000-1 de manera conjunta.

Integrar la norma ISO/IEC 27001 vigente dentro del sistema de gestión implementado con la ISO/IEC 20000-1.

Versión en inglés: Publicada en Octubre de 2012.

Versión en español: No se tiene registro de versiones traducidas.

ISO/IEC 27014 - Guía para la Administración Corporativa de la seguridad de la información.

Proporciona una orientación sobre los conceptos y principios para Administración de la seguridad de la información, mediante el cual las organizaciones pueden evaluar, dirigir, controlar y comunicar las actividades relacionadas con la seguridad de la información dentro de la organización.

Es aplicable a todos los tipos y tamaños de organizaciones

Versión en inglés: Publicada en Mayo de 2013.

Versión en español: No se tiene registro de versiones traducidas

ISO/IEC 27015 - Proporciona una orientación que complementa las directrices definidas en la norma ISO/IEC 27002 para iniciar, implementar, mantener y mejorar la seguridad de la información dentro de las organizaciones que prestan servicios financieros y de seguros.

Versión en inglés: Publicada en Noviembre de 2012.

Versión en español: No se tiene registro de versiones traducidas

ISO/IEC 27016 - Valoración de los aspectos financieros de la seguridad de la información.

Esta norma se encuentra en fase de desarrollo, por lo que aún no se dispone de ninguna versión de esta norma.

ISO/IEC 27017 - Guía de seguridad para Cloud Computing.

Esta norma se encuentra en fase de desarrollo, por lo que aún no se dispone de ninguna versión de esta norma.

ISO/IEC 27018 - Código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

Esta norma se encuentra en fase de desarrollo, por lo que aún no se dispone de ninguna versión de esta norma.

ISO/IEC 27019 - Establece las directrices basados en la norma ISO/IEC 27002 para la gestión de seguridad de la información aplicada a los sistemas de control de procesos y la tecnología de automatización que se utilizan en la industria de servicios públicos de energía.

Cubre los sistemas utilizados para el control y seguimiento de la producción, transporte, almacenamiento y distribución de energía eléctrica, gas y calor, en combinación con el control de los procesos de apoyo. Esto incluye: los sistemas de administración, unidades de programación y parametrización, los sistemas informáticos utilizados para su funcionamiento, controladores digitales, componentes de automatización, dispositivos de control, sensores digitales, elementos actuadores automatizados, dispositivos de medición digital, sistemas de protección y seguridad digitales, la tecnología de la comunicación utilizada en el dominio de control de procesos, la tecnología de control remoto, el software, firmware y las aplicaciones instaladas en los sistemas mencionados.

Quedan fuera del ámbito de esta norma, los equipos de control convencional que no son digitales, es decir, sistemas de monitoreo y control de procesos puramente mecánicos o electromecánicos, así como los sistemas de control de procesos de energía en los hogares o edificios residenciales privados.

Versión en inglés: Publicada en Julio de 2013.

Versión en español: No se tiene registro de versiones traducidas

ISO/IEC 27031 - Describe los conceptos y principios de la tecnología de información y comunicación (TIC) y la preparación de una organización para mantener la continuidad del negocio. Proporciona un marco de métodos y procesos para identificar y especificar los aspectos tales como: criterios de rendimiento, diseño, puesta en marcha, gestión, planificación y mejora continua de las TICs implementadas en una organización, con la idea que sus servicios e infraestructuras estén listas para apoyar las operaciones del negocio en caso de presentarse eventos e incidentes, los cuales podrían afectar la infraestructura y las funciones críticas del negocio, incluida la seguridad. El documento toma como referencia el estándar BS 25777. Se aplica a cualquier organización pública o privada, independientemente de su tamaño. También permite a una organización medir los parámetros de rendimiento de una manera consistente y reconocida.

Versión en inglés: Publicada en Marzo de 2011.

Versión en español: No se tiene registro de versiones traducidas

ISO/IEC 27032 - Guía de orientación para la mejora del estado de seguridad cibernética.

Proporciona una guía para mejorar el estado de la seguridad cibernética, extrayendo los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad, en particular: seguridad de la información, seguridad de la red, seguridad en Internet, y protección de infraestructuras críticas de información (PICI).

Cubre las prácticas de seguridad de línea de base para los interesados en el ciberespacio. Proporciona una visión general de la Seguridad Cibernética, una explicación de la relación entre Ciberseguridad y otros tipos de seguridad, una orientación para abordar las cuestiones de seguridad cibernética comunes, y un marco que permitirá a los interesados colaborar en la resolución de temas de seguridad cibernética.

Versión en inglés: Publicada en Julio de 2012.

Versión en español: No se tiene registro de versiones traducidas

ISO/IEC 27033 - Parcialmente desarrollada, está dedicada a la Seguridad en Redes, consta de siete partes.

27033-1 Conceptos generales

Es una visión general de seguridad de la red y los conceptos asociados. Proporciona una orientación sobre la manera de identificar y analizar los riesgos de seguridad de red, y la definición de los requisitos de seguridad de la red, aplicables a la seguridad de los dispositivos, aplicaciones/servicios, y los usuarios finales, además de la seguridad de la información que se transfiere a través de los enlaces de comunicación.

Es relevante para cualquier entidad que posee o utiliza una red de datos, dando un énfasis a los Administradores que tienen responsabilidades específicas para la seguridad de la información, seguridad y funcionamiento de la red, programa de seguridad general de la organización y el desarrollo de políticas de seguridad.

En general, se ofrece una visión general de la serie ISO / IEC 27033 y una " hoja de ruta " para todas las demás partes.

Versión en inglés: Publicada en Diciembre de 2009.

Versión en español: No se tiene registro de versiones traducidas

27033-2 Directrices de diseño e implementación de seguridad en redes.

Da las pautas a las organizaciones para planificar, diseñar e implementar la seguridad de los documentos en la red.

Versión en inglés: Publicada en Julio de 2012.

Versión en español: No se tiene registro de versiones traducidas

27033-3 Escenarios de referencia de redes.

Se centrará en la revisión técnica de la arquitectura/opciones de diseño de las redes, de conformidad con las normas ISO/IEC 27033-2, ISO/IEC 27033-4 e ISO/IEC 27033-6; dependerá de las características del entorno de red en revisión, es decir, la situación en particular de la red. Para cada escenario, se proporciona orientación detallada sobre las amenazas de seguridad y las técnicas de diseño de seguridad y los controles necesarios para mitigar los riesgos asociados.

Versión en inglés: Publicada en Diciembre de 2010.

Versión en español: No se tiene registro de versiones traducidas

27033-4 Aseguramiento de las comunicaciones entre redes mediante gateways de seguridad.

Se encuentra en desarrollo, aún no ha sido publicada.

27033-5 Aseguramiento de comunicaciones mediante VPNs.

Proporciona directrices para la selección, implementación y monitoreo de los controles técnicos necesarios para garantizar la seguridad de la red mediante conexiones VPN (Red Privada Virtual) para interconectar las redes y conectar a los usuarios remotos a las redes.

Versión en inglés: Publicada en Agosto de 2013.

Versión en español: No se tiene registro de versiones traducidas

27033-6 Convergencia IP.

Se encuentra en desarrollo, aún no ha sido publicada.

27033-7 Redes inalámbricas.

Se encuentra en desarrollo, aún no ha sido publicada.

ISO/IEC 27034 - Dedicada a la seguridad en aplicaciones informáticas, consta de cinco partes.

27034-1 Conceptos generales. Presenta una visión general de seguridad de la aplicación. Introduce definiciones, conceptos, principios y procesos que intervienen en la seguridad de aplicaciones. (publicada el 21 de Noviembre de 2011)

27034-2 Marco normativo de la organización (aún en desarrollo).

27034-3 Proceso de gestión de seguridad en aplicaciones. (aún en desarrollo).

27034-4 Validación de la seguridad en aplicaciones. (aún en desarrollo).

27034-5 Estructura de datos de protocolos y controles de seguridad de aplicaciones. (aún en desarrollo).

Versión en inglés: La norma de encuentra parcialmente desarrollada. La primera parte ISO/IEC 27034-1 fue publicada en Noviembre de 2011.

Versión en español: No se tiene registro de versiones traducidas.

ISO/IEC 27035 – Proporciona una guía sobre la gestión de incidentes de seguridad en la información para organizaciones grandes y medianas.

Dentro de su estructura puede realizar las siguientes actividades:

Detectar, informar y evaluar los incidentes de seguridad de la información.

Responder y gestionar los incidentes de seguridad de la información.

Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información.

Mejorar continuamente la seguridad de la información y la gestión, como resultado de la evaluación de los incidentes de seguridad de la información y las vulnerabilidades.

Las organizaciones más pequeñas pueden utilizar un conjunto básico de documentos, procesos y rutinas que se describen en esta Norma,

dependiendo de su tamaño y tipo de negocio en relación a la situación de riesgo para la seguridad de la información.

Versión en inglés: Publicada en Septiembre de 2011.

Versión en español: No se tiene registro de versiones traducidas.

ISO/IEC 27036 - Guía para la seguridad en las relaciones con proveedores. La norma se encuentra parcialmente desarrollada, consta de cuatro partes.

27036-1 Visión general y conceptos.

27036-2 Requisitos comunes.

27036-3 Seguridad en la cadena de suministro TIC.

27036-4 Seguridad en outsourcing (externalización de servicios).

Al momento la única parte que ya se ha publicado es la ISO/IEC 27036-3.

Versión en inglés: ISO/IEC 27036-3 Publicada en Noviembre de 2013.

Versión en español: No se tiene registro de versiones traducidas

ISO/IEC 27037 Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio en el intercambio entre las diferentes jurisdicciones.

Proporciona orientación a las personas con respecto a las situaciones comunes que se encuentran en todo el proceso de manejo de la evidencia digital y ayuda a las organizaciones en sus procedimientos disciplinarios para facilitar el intercambio de potencial evidencia digital entre jurisdicciones.

Entre los dispositivos incluidos en esta norma podemos nombrar los siguientes:

Medios de almacenamiento digital utilizados en los ordenadores estándar como discos duros, disquetes, discos ópticos y magneto-ópticos, dispositivos de datos con funciones similares.

Los teléfonos móviles, asistentes personales digitales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria.

Sistemas de navegación móvil.

Digitales y cámaras de vídeo (incluyendo CCTV).

Equipo estándar con conexiones de red.

Las redes basadas en TCP / IP y otros protocolos digitales.

Los dispositivos con funciones similares a las anteriores.

Versión en inglés: Publicada en Octubre de 2012.

Versión en español: No se tiene registro de versiones traducidas

ISO/IEC 27038 - Guía de especificación para seguridad en la redacción digital.

En fase de desarrollo, aún no ha sido publicada.

ISO/IEC 27039 - Guía para la selección, despliegue y operatividad de sistemas de detección y prevención de intrusión (IDS/IPS).

En fase de desarrollo, aún no ha sido publicada.

ISO/IEC 27040 - Guía para la seguridad en medios de almacenamiento.

En fase de desarrollo, aún no ha sido publicada.

ISO/IEC 27041 - Guía para garantizar la idoneidad y adecuación de los métodos de investigación.

En fase de desarrollo, aún no ha sido publicada.

ISO/IEC 27042 - Guía con directrices para el análisis e interpretación de las evidencias digitales.

En fase de desarrollo, aún no ha sido publicada.

ISO/IEC 27043 - Desarrollará principios y procesos de investigación.

En fase de desarrollo, aún no ha sido publicada.

ISO/IEC 27044 - Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).

En fase de desarrollo, aún no ha sido publicada.

ISO/IEC 27799 - Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

Versión en inglés: Publicada en Julio de 2008.

Versión en español: Traducida para España (UNE-ISO/IEC 27799), versión de enero de 2010.

Proceso para obtener la certificación ISO/IEC 27001

El hecho de disponer de la certificación según ISO 27001 le ayuda a cualquier organización a gestionar y proteger su información. La norma es adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. Es particularmente interesante si la protección de la información es crítica, como en los sectores financieros, Salud, sectores públicos y tecnología de la información (TI).

De las series que conforman la familia ISO 2700, la serie ISO 27001 es la única norma que brinda una certificación internacional auditable que define los requisitos para un SGSI.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes.

Beneficios de la certificación ISO 27001

Puede aportar las siguientes ventajas a una organización:

Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.

Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.

Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.

Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.

Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.

El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

Pasos hacia la certificación

1. Elegir la norma: Antes iniciar los contactos con las empresas auditoras, es necesario familiarizarse con la norma por lo que es necesario adquirir la norma, leerla y familiarizarse con ella.

2. Contactar a un auditor calificado que será la persona o entidad encargada de analizar los requerimientos de la organización. Con esta evaluación previa se podrá tener una idea del costo y tiempo necesario para implementar o adecuar un SGSI conforme la normativa ISO 27001. El Auditor debe tener la capacidad técnica necesaria para identificar cualquier omisión o punto débil que deba resolverse antes de la auditoría formal. En caso que el auditor encuentre áreas de incumplimiento, la organización tiene un plazo para adoptar medidas correctivas, sin perder la vigencia de la certificación (en caso de tenerla) o la continuidad en el proceso de certificación. La Organización debe contar con el soporte técnico adecuado para cumplir los requerimientos necesarios para implementar, mejorar y mantener el SGSI.

   Dentro de esta revisión, de forma conjunta (Administradores – Auditor – Departamento Técnico), se debe analizar:

   La definición y alcance,

   Análisis de los objetivos a alcanzar al implementar ISO 27000

   Inventario de activos

   Análisis de Riesgos seguridad información

   Definición Controles

   Implementación Controles

   Concienciación y socialización sobre la importancia de mantener un SGSI a los miembros de la organización.

3. Auditoría Final: Una vez concluida satisfactoriamente la auditoría, el Auditor emite un certificado de conformidad con la norma ISO 27001. El certificado tiene una validez de tres años y el auditor le visitará regularmente para ayudarle a garantizar que continúa cumpliendo con los requisitos y para apoyarle en la mejora continua de los SGSI.

Estado de las normas iso 27000 en Ecuador

Con el apoyo de varios Ministerios e Instituciones del Sector Público, desde el año 2010, se ha procurado definir los lineamientos que regularicen la implementación de SGSIs en nuestro País.

De esta forma, de acuerdo a la información que se muestra en la página Web del Instituto Ecuatoriano de Normalización (INEN), en el periodo 2010-2011el Subcomité Técnico de "Tecnologías de La Información" había propuesto al menos 7 normas de la familia ISO 2700 para que sean adoptadas como normativa Ecuatoriana, las cuales han sido revisadas por los Ministerios de Telecomunicaciones, Ministerio de Industrias y Productividad, Subsecretaría de Industrias, Productividad e Innovación Tecnológica.

Mediante Acuerdos Ministeriales publicados en el Registro Oficial No. 804 del 29 de julio de 2011 y No. 837 del 19 de agosto de 2011, La Secretaría Nacional de Administración Pública crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, dentro de sus atribuciones tiene la responsabilidad de establecer los lineamientos de seguridad informática, protección de infraestructura computacional, incluyendo la información contenida, para las entidades de la

Administración Pública Central e Institucional. En respuesta a esta tarea, La Comisión desarrolla el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la Norma NTE INEN-ISO/IEC 27002 (Traducción de la norma ISO/IEC 27000).

De igual forma, mediante resoluciones Ministeriales, publicadas en el Registro Oficial, han sido revisadas y aprobadas varias Normas Técnicas Ecuatorianas, entre las que se incluyen:

NTE INEN-ISO/IEC 27000, basada en la norma ISO/IEC 27000, publicada en el Registro Oficial 699 del 09 de mayo de 2012.

NTE INEN-ISO/IEC 27001, basada en la norma ISO/IEC 27001, publicada en el Registro Oficial 491 del 14 de julio de 2011.

NTE INEN-ISO/IEC 27002, basada en la norma ISO/IEC 27002, publicada en el Registro Oficial 596 del 22 de mayo de 2009.

NTE INEN-ISO/IEC 27003, basada en la norma ISO/IEC 27003, publicada en el Registro Oficial 699 del 09 de mayo de 2012.

NTE INEN-ISO/IEC 27004, basada en la norma ISO/IEC 27004, publicada en el Registro Oficial 699 del 09 de mayo de 2012.

NTE INEN-ISO/IEC 27005, basada en la norma ISO/IEC 27005, publicada en el Registro Oficial 699 del 09 de mayo de 2012.

NTE INEN-ISO/IEC 27006, basada en la norma ISO/IEC 27003, publicada en el Registro Oficial 654 del 06 de marzo de 2012.

NTE INEN-ISO/IEC 27033-1, basada en la norma ISO/IEC 27033-1, se encuentra aprobada por el INEN desde el año 2012, sin embargo no se tiene información si han sido publicadas en el Registro Oficial.

NTE INEN-ISO/IEC 27799, basada en la norma ISO/IEC 27799, se encuentra aprobada por el INEN desde el año 2012, sin embargo no se tiene información si han sido publicadas en el Registro Oficial.

Con estos antecedentes y contando con una Normativa Nacional Vigente, el Gobierno Ecuatoriano, dispone a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, el uso obligatorio de las Normas Técnicas Ecuatorianas serie NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. Esta disposición fue publicada en el Segundo Suplemento del Registro Oficial 088 del 19 de septiembre de 2013.

Esto implica que las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, tienen un plazo de 18 meses para implementar el EGSI, las normas marcadas como prioritarias deberán implementarse en un periodo de 6 meses.

La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

La entidad encargada de realizar el seguimiento y control anual, o cuando las circunstancias lo ameriten, será La Secretaría Nacional de la Administración Pública, de conformidad a los lineamientos de la norma INEN ISO/IEC 27002 y sus futuras modificaciones, lo que implica que las entidades de la Administración Pública y que dependen de la Función Ejecutiva deberán realizar una evaluación, una adecuación o implementación, un seguimiento y una mejora continua sobre sus Sistemas de Gestión de Seguridad de la Información.

Una de las primeras Instituciones públicas en implementar esta normativa en nuestro País, es la Corporación Nacional de Telecomunicaciones con su proyecto “Diseño e implementación del Sistema de Gestión de Seguridad de la Información” (SGSI) aplicado al proceso: Venta e Instalación de Productos y Servicios de Datos e Internet para Clientes Corporativos”.

Conclusiones

Hemos analizado la situación actual de las normas que componen la serie ISO/IEC 27000, con lo que se ha podido comprobar que cada norma tiene un campo de aplicación específico dependiendo del sector, tamaño de la empresa, tipo de tecnología de comunicación que utilizan, aplicaciones y servicios que ofrecen, entre otras.

Hemos conocido que las normas se pueden conseguir en sus versiones originales en idioma inglés, sin embargo algunas normas pueden conseguirse en idioma español y que algunas de ellas se encuentran en proceso de preparación.

En el ámbito Nacional, hemos conocido que en el Ecuador, se ha impulsado la aprobación de la normativa serie ISO/IEC 27000, pero por el momento se ha dado énfasis a la implementación de la Seguridad de la Información en las Instituciones Públicas o las que están relacionadas con la Función Ejecutiva.

1.1.1.1.1 Fuentes y Referencias Bibliográficas

Fundación Wikipedia Inc, Serie de normas ISO/IEC 27000, agosto.20.2013, http://es.wikipedia.org/wiki/ISO/IEC_27000-series

IEC – Webstore de la Comisión Electrotécnica Internacional, Preview de las normas ISO serie 27000 publicadas - versión original - incluyen Abstract – Introducción e Indice, 2013, http://webstore.iec.ch

Agustín López Neira & Javier Ruiz Spohr – Portal en español de la norma ISO 2700, Sistema de Gestión de la Seguridad de la Información, http://www.iso27000.es/sgsi.html

Agustín López Neira & Javier Ruiz Spohr – Portal en español de la norma ISO 2700, Serie ISO 27000, http://www.iso27000.es/sgsi.html

The ISO 27000 Directory- , A Short History of the ISO 27000 Standards, 2007, http://www.27000.org/thepast.htm

The ISO 27000 Directory- , An Introduction to ISO 27001, ISO 27002....ISO 27008, 2013, http://www.27000.org/thepast.htm

Revista Ekos Negocios, Roberto Chávez, ERS (Enterprise Risk Services), Noticias empresariales Ecuador: "Deloitte explicó a entidades públicas los lineamientos para la ejecución de la norma de seguridad 2014", Noviembre.29.2013, http://www.ekosnegocios.com/negocios/m/verArticulo.aspx?idart=2703&c=1

The British Standards Institution - España, Seguridad de la Información ISO 27001 – Auditoria y Certificación, 2013, http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion

Instituto Ecuatoriano de Normalización - Subcomité Técnico de "Tecnologías de la Información", Normas propuestas para el proyecto de Regulación de las TIC's, Normas de Seguridad, 2011, http://www.inen.gob.ec/index.php?option=com_content&view=article&id=163&Itemid=154

Instituto Ecuatoriano de Normalización - Normas Técnicas Ecuatorianas NTE INEN ISO, ISO/IEC aprobadas por el Subcomité Técnico de Tecnologías de la Información, 2012, http://www.inen.gob.ec/images/pdf/normaliza/NTE%20aprobadas%20SCT%20TIC%202012.pdf

Registro Oficial de la República de Ecuador, No. 699 del 09 de mayo de 2012, Ministerio de Industrias y Productividad, Subsecretaría de la Calidad, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27000, NTE-INEN-ISO/IEC 27003, NTE-INEN-ISO/IEC 27004, NTE-INEN-ISO/IEC 27005.

Registro Oficial de la República de Ecuador, No. 491 del 14 de julio de 2011, Ministerio de Industrias y Productividad, Subsecretaría de Industrias, Productividad e Innovación Tecnológica, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27001.

Registro Oficial de la República de Ecuador, No. 596 del 22 de mayo de 2009, Instituto Ecuatoriano de Normalización, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27002.

Registro Oficial de la República de Ecuador, No. 654 del 06 de marzo de 2012, Ministerio de Industrias y Productividad, Subsecretaría de la Calidad, Aprobación y oficialización de la norma NTE-INEN-ISO/IEC 27006.

Registro Oficial de la República de Ecuador, No. 88 del 19 de septiembre de 2013 (segundo suplemento), Función Ejecutiva de la República del Ecuador, Acuerdo Ejecutivo No. 166 del 19 de septiembre de 2013, Secretaría Nacional de la Administración Pública, Disposición a las Entidades de la Administración Pública Central, Institucional y que dependan de la Función Judicial el uso obligatorio de las Normas NTE INEN ISO/IEC 27000. Implementación del EGSI.